



AEROSPACE RECOMMENDED PRACTICE

ARP5107™

REV. C

Issued 1997-06
Revised 2018-09

Superseding ARP5107B

Guidelines for Time-Limited-Dispatch (TLD) Analysis for Electronic Engine Control Systems

RATIONALE

This standard has been revised to harmonize its content with EASA CM-MMEL-001 and reflect new methodologies in the field.

TABLE OF CONTENTS

1.	SCOPE.....	4
1.1	Purpose.....	4
1.2	Summary of Revisions.....	4
1.2.1	Summary of Revision A.....	4
1.2.2	Summary of Revision B.....	5
1.2.3	Summary of Revision C.....	5
1.3	Field of Application.....	6
2.	REFERENCES.....	6
2.1	Applicable Documents.....	6
2.1.1	FAA Publications.....	6
2.1.2	EASA Publications.....	6
2.2	Acronyms and Symbols.....	6
3.	APPLICABILITY.....	8
4.	HISTORICAL PERSPECTIVE.....	8
5.	INTEGRITY GUIDELINES.....	8
6.	GENERAL ANALYSIS APPROACH.....	10
6.1	FADEC System Configuration.....	10
6.2	Clarification and Management of Aircraft and Engine Control Faults Categories.....	11
6.3	Repair Categories: Immediate, Short, and Long Time.....	12
6.4	Classification of FADEC Fault Types.....	13
6.4.1	No Dispatch (ND) Type Faults.....	13
6.4.2	Short Time (ST) Type Faults.....	13
6.4.3	Long Time (LT) Type Faults.....	14
6.4.4	"Applicant Defined Dispatch" or "Engine Manufacturer/Airframer Convenience".....	14
6.4.5	Combinations of Faults and Undetected (UC) Faults.....	14
6.4.6	Aircraft Related Information.....	15
6.5	Recommendations on Items Considered Part of the FADEC System.....	15
6.6	Recommendations on In-Service LOTC Reporting.....	22

SAE Technical Standards Board Rules provide that: "This report is published by SAE to advance the state of technical and engineering sciences. The use of this report is entirely voluntary, and its applicability and suitability for any particular use, including any patent infringement arising therefrom, is the sole responsibility of the user."

SAE reviews each technical report at least every five years at which time it may be revised, reaffirmed, stabilized, or cancelled. SAE invites your written comments and suggestions.

Copyright © 2018 SAE International

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior written permission of SAE.

TO PLACE A DOCUMENT ORDER: Tel: 877-606-7323 (inside USA and Canada)
Tel: +1 724-776-4970 (outside USA)
Fax: 724-776-0790
Email: CustomerService@sae.org
http://www.sae.org

SAE WEB ADDRESS:

**SAE values your input. To provide feedback on this
Technical Report, please visit
<http://standards.sae.org/ARP5107C>**

7.	CALCULATION APPROACHES - SINGLE ENGINE ANALYSIS.....	22
7.1	A Simple Time-Averaging Approach.....	22
7.1.1	LOTIC Rate for Full-up Electronics.....	25
7.1.2	Average LOTIC Rate for Short Time (ST) Faults.....	25
7.1.3	Average LOTIC Rate for Long Time (LT) Faults.....	26
7.1.4	Calculations of the Average LOTIC Rate Using the TWA Approach.....	26
7.1.5	An Example Calculation.....	27
7.2	Markov Model Approach.....	28
7.2.1	Open Loop Markov Models.....	28
7.2.2	Closed Loop Markov Model Approach.....	32
7.2.3	Examples of Single Fault States.....	37
7.2.4	Acceptability (and Accuracy) of Single State Models.....	37
7.3	Comparison of TWA and MM Approaches.....	37
7.4	A Single State FADEC System MM Example.....	38
7.4.1	Description of the Excel Spreadsheet Data.....	38
7.4.2	Validity of the Calculated Data.....	47
7.5	Second Example: A Single and Dual State Model of a FADEC System.....	48
7.6	Discussion of Markov Model and TWA Approaches, and the Use of Fault Trees (for Determining LOTIC Rates When Operating with Faults).....	48
7.7	Time-Since-Fault (i.e., On-Condition) Repair Versus Periodic Inspection and Repair.....	51
8.	CALCULATION APPROACHES - DUAL ENGINE ANALYSIS.....	55
8.1	Time-Averaging Approach.....	55
8.2	Maximum Specific Risk Failure Rates as a Function of Dispatch Configuration.....	55
9.	SUMMARY.....	56
10.	NOTES.....	57
10.1	Revision Indicator.....	57
APPENDIX A	EARLY APPLICATIONS.....	58
APPENDIX B	DISCUSSION OF SOME TYPICAL FADEC SYSTEM FAULTS AND THEIR APPLICABILITY TO THE LOTIC ANALYSIS.....	59
APPENDIX C	DISCUSSION OF THE MMEL, DDG, CMRS, AND THEIR RELATIONSHIP TO FADEC SYSTEM MAINTENANCE (THE HANDLING OF ND, ST, AND LT FAULTS).....	61
APPENDIX D	PROBABILITY OF A DUAL ENGINE FAILURE WITH DIVERSION AND TURNBACK.....	64
APPENDIX E	REVIEW OF THE COEFFICIENTS USED IN THE TIME-WEIGHTED-AVERAGE (TWA) EQUATION.....	66
APPENDIX F	WHEN IS A SINGLE STATE MODEL OK?.....	71
APPENDIX G	COMPARISON OF THE ASYMPTOTIC VALUE OF $\{(DP/DT)/(1 - P)\}$ IN AN OPEN LOOP MARKOV MODEL WITH THAT OF THE AVERAGE FAILURE RATE OF THE SYSTEM FROM A CLOSED LOOP MARKOV MODEL.....	74
Figure 1	Simplified FADEC system.....	11
Figure 2	Simplified FADEC system fault diagram.....	14
Figure 3A	Simplified flow diagram for FADEC system faults leading to LOTIC.....	15
Figure 3B	Illustrations of all LOTIC events, all IFSD events, and engine control system elements involved in a TLD analysis.....	17
Figure 4	A graphical representations of the failure paths of a simple FADEC system that lead to LOTIC.....	23
Figure 5	Plot of the LOTIC rate for the example data given in 7.1.5 for both the original fractional coefficients (as given in the original ARP) with the improved fractional coefficients given in this revised ARP.....	28
Figure 6	Open loop Markov model water fall diagram.....	29
Figure 7	Open loop Markov model of simple FADEC system with repair for short and long time fault states.....	29
Figure 8	Probability flow into and out of state P_j	30
Figure 9	Closed loop MM for simple FADEC control system with repair for short and long term fault states.....	32
Figure 10	Single state Markov model.....	34

Figure 11	Comparison of TWA solutions using the original ARP fractional coefficients and the balanced Equation 6 coefficients of this ARP with Markov model solutions using Equations 20, 20c, and 20f (from this ARP) for the FADEC system data given in 7.1.5.....	39
Figure 12	MM diagram of a typical FADEC system (Note: All λ 's are failures per million hours)	40
Figure 13A	LOTC rate (Table 1 data using Equation 20) as a function of the LT fault repair time for simple FADEC system example of Figure 12	45
Figure 13B	Comparison of Figure 12 Markov model LOTC calculations Using Equations 20, 20c, and 20f.....	46
Figure 14	Second example of single state Markov model of a typical FADEC system, with 23 single fault states	49
Figure 15	Figure 14 model with 180 dual states added	50
Figure 16	LOTC rates as a function of LT repair time for both the single and dual state models of Figures 14 and 15	51
Figure 17	($T_{\text{INSPECT}}/T_{\text{TSF}}$) versus ($T_{\text{TSF}}/T_{\text{MTBF(LT)}}$)	53
Figure 18	Derivation of approximation given in Equation 24	54
Table 1	Typical categorization of FADEC system elements	18
Table 2	Spreadsheet solution for FADEC system example shown in Figure 12	41
Table 3	Spread sheet showing the calculations for determining the coefficients a_0 , a_1 , b_0 , b_1 , c_0 , c_1 , d_0 , and d_1 used in Equation 20c	47
Table 4	Dual engine specific risk as a function of dispatch configuration	56

1. SCOPE

This SAE Aerospace Recommended Practice (ARP) provides methodologies and approaches which have been used for conducting and documenting the analyses associated with the application of Time Limited Dispatch (TLD) to the thrust control reliability of Full Authority Digital Engine Control (FADEC) systems. The TLD concept is one wherein a fault-tolerant system is allowed to operate for a predetermined length of time with faults present in the redundant elements of the system, before repairs are required. This document includes the background of the development of TLD, the structure of TLD that was developed and implemented on present generation commercial transports, and the analysis methods used to validate the application of TLD on present day FADEC equipped aircraft. Although this document is specific to TLD analyses (for FADEC systems) of the loss of thrust control, the techniques and processes discussed in this document are considered applicable to other FADEC system failure effects or other systems, such as: thrust reverser, and propeller control systems, and overspeed protection systems.

1.1 Purpose

The purpose of this document is to provide guidance on achieving approval of time-limited-dispatch (TLD) for full authority digital engine control (FADEC) systems. TLD addresses continued operational safety with faults already detected (by fault detection function, crew, or maintenance activity) and not yet repaired. In this regard, the usage of the term "TLD" refers to the concept that FADEC engine control systems shall be allowed to operate with faults for a specified period of time, after which appropriate repairs shall be made to bring the system back to a "full up" configuration. For the purposes of this document, the term "full up" is used to indicate that the FADEC system is free of faults which affect its loss of thrust control (LOTC) failure rate, as defined in Section 5. Hence, "required repairs" for this application of TLD are limited to only those faults that affect the LOTC rate, and faults that do not affect the LOTC rate, such as faults in sensors used for engine condition monitoring, are not addressed in these guidelines. Sensors that could affect the LOTC rate, such as oil pressure, oil temperature, and exhaust gas temperature (EGT) should be included in the analysis if those sensors are part of the engine's FADEC system.

This document is primarily concerned with LOTC events which are caused by failures and/or faults in the engine's control system. Engine failures from any other causes are not the subject of these guidelines, but failures that may affect MMEL activities outside of the engine should be identified. In addition, this document is not intended to establish specific requirements for FADEC system certification or design. Specific requirements pertaining to certification should be coordinated with the appropriate certifying agency.

1.2 Summary of Revisions

1.2.1 Summary of Revision A

A significant improvement in determining the fractional coefficients of the time-weighted-average (TWA) equation, which is the first approach described herein for estimating the average LOTC rate of the system, has been made and is described in 7.1. The new coefficients allow the TWA method to yield a more balanced solution - one which is closer to the Markov model solution and somewhat simpler to use.

Much has changed in the description of the Markov modeling (MM) analysis approach described in this revision. Since the original release in June, 1997, the authors of this ARP have a better understanding of the MM approach as it applies to FADEC as well as other systems. Unique to this document is the description of MM as either an Open Loop or Closed Loop model. The nomenclature of Open Loop and Closed Loop Markov models is unique to this document. The authors have not seen this terminology used elsewhere, and there is no intention herein to set any type of standard in the using of this terminology. The development of the Closed Loop MM approach has led to not having to solve a set of differential equations to obtain the steady state solution for the overall average failure rate of a system, but rather, simply solving a set of algebraic equations to obtain the solution. This was implied in the original release, because the MMs in that release were solved by integrating the differential equations until a steady state solution was obtained, where all the time derivatives were essentially zero. However, it was not specifically called out that the derivatives should be set to zero at the onset, and the resulting set of algebraic equations solved to obtain the values of the state probabilities.

In addition, it was not recognized that the values obtained for the state probabilities, which are dependent on the value of the feedback rate from the fully-failed, loss-of-thrust-control (LOTC) state to the full-up state, do not affect the failure rate of the system. Hence, although the original release provides some rationale for setting the feedback or repair rate from the fully failed LOTC state to the full-up state to unity (i.e., 1.0), the value of this feedback rate doesn't matter and the rationale for setting the feedback rate to unity can be misleading. As the new material shows, the solution is independent of all state probabilities and the value of the fully failed to full-up feedback rate. The solution is only dependent on the failure rates between the various states of the model and the repair rates used for the short time (ST), long time (LT) states, and if modeled, any no-dispatch (ND) fault states.

Experience has also shown that simulating states representing two or more failures has little influence on the overall LOTC rate of FADEC systems when the repair rates for the various fault states are much more frequent than the failure rates into and out of those fault states. When this is the case, constructing a "single state model" is usually adequate. In single state models, described in 7.2.2.3, only single fault states are modeled, and only those additional single failures that would cause the control system to go from those single fault states to the LOTC state are modeled. Adding additional multiple failure states only affects the answer by small amount, i.e., less than 5%. This is discussed in more detail in Appendix G.

Similar to the above, the use of the terminology "single state model" is unique to this document, and there is no intention to set any terminology standard with the use of this descriptive term. Some who have reviewed this document have commented that the use of the terminology single state model is misleading because a single state model actually models all dual failures that lead to the LOTC state. This is correct. However, the selection of the terminology was made because the model explicitly shows only the single failure states. All dual failures that lead to LOTC events are included in the LOTC failure state, and no dual failures that do NOT result in an LOTC event are modeled.

Revision A of this document aligned with the R1 revision to PS-ANE100-2001-1993-33.28TLD-R1, Policy for Time Limited Dispatch (TLD) of Engines Fitted with Full Authority Digital Engine Controls (FADEC) Systems.

A discussion of the elements that are considered part of the engine control system and should be represented in the LOTC analysis (see 6.5).

1.2.2 Summary of Revision B

Section 6.4, on Recommendations on Items Considered Part of the FADEC System, has been significantly expanded to provide more guidance on that subject. Section 6.6, on Recommendations on In-Service LOTC Reporting, has been added.

The functions of the system, the elements selected for use in the system, and the design implementation all depend on the overall system architecture. In addition, integration between the engine and the aircraft control systems is constantly changing. All of these factors impact the selection of the elements to include as part of the FADEC system. Therefore, the information included in this section does not provide an absolute answer, but is intended to provide a methodology to use in selecting which elements of the aircraft/engine control system should be included in the analysis.

The added Table 1 in that section illustrates how to consider all elements of the thrust or power control system, the functions and failure modes associated with the element, and then evaluate whether it is or is not part of the TLD restriction envelope depicted in Figure 3B. The table also shows the most likely result of a failure of the element by identifying the applicable area of Figure 3B.

1.2.3 Summary of Revision C

Due to the increased complexity of Engine Control integration into airframe systems, and a tendency of aircraft and engine functions to be interdependent, Engine Control TLD analyses have evolved to address functions that are not purely a function of engine controls.

Following the introduction of new EASA Part-21 requirements on Operational Suitability Data (OSD), EASA has published CM-MMEL-001 to clarify how compliance to the OSD certification basis for MMEL should be conducted by the aircraft applicant on MMEL items already subject to a TLD analysis. The referenced CM addresses EASA's concern of including airframe systems in the Engine Control TLD analysis. The intent of this inclusion is to address dispatch capability of the aircraft in a similar manner as the engine controls related items (e.g., same FADEC Short Term alert message in the cockpit). An alignment activity has been conducted between the SAE E-36 Electronic Engine Controls Committee and EASA for this version of ARP5107. Section 6.2 has been added to provide guidance on clarifying which functions are solely engine related, and which are part of other airframes systems in the TLD analysis.

1.3 Field of Application

This document applies to fault-tolerant (or redundant) FADEC control systems for aircraft engines on multi-engine aircraft. TLD addresses the level of degraded resource that is allowable - while still meeting the necessary airworthiness requirements - for FADEC controlled aircraft engines used on multi-engine aircraft. (It is noted that the submittal of a TLD analysis is not a requirement for certification of an engine incorporating a FADEC system. The analysis is a means to substantiate and obtain approval for dispatching and operating a FADEC system - for limited time periods - with faults present in the system.) Although this document specifically applies to FADEC systems on multi-engine aircraft, the methodologies presented herein with regard to achieving an overall average system failure rate can also be applied to other systems.

2. REFERENCES

2.1 Applicable Documents

The following publications form a part of this document to the extent specified herein. The latest issue of SAE publications shall apply. The applicable issue of other publications shall be the issue in effect on the date of the purchase order. In the event of conflict between the text of this document and references cited herein, the text of this document takes precedence. Nothing in this document, however, supersedes applicable laws and regulations unless a specific exemption has been obtained.

2.1.1 FAA Publications

Available from Federal Aviation Administration, 800 Independence Avenue, SW, Washington, DC 20591, Tel: 866-835-5322, www.faa.gov.

- (Original) ANE Policy Letter, dated October 28, 1993, Time-Limited-Dispatch of Engines Fitted with FADEC Systems
- Policy Memorandum, PS-ANE100-2001-1993-33.28TLD-R1, Policy for Time Limited Dispatch (TLD) of Engines Fitted with Full Authority Digital Engine Controls (FADEC) Systems, June 29, 2001
- Advisory Circular, AC 33.28-3, "Compliance Criteria for 14 CFR §33.28, Aircraft Engines, Electrical and Electronic Engine Control Systems", issued May 23rd., 2014

2.1.2 EASA Publications

Available from European Aviation Safety Agency, Ottoplatz, 1, D-50679 Cologne, Germany, Tel: +49 221 8999 000, www.easa.europa.eu

AMC 20-3	Certification of Engines Equipped with Electronical Engine Control Systems
CM-MMEL-001 Issue 1	Engine Time Limited Dispatch and Master Minimum Equipment List (MMEL)
CS-E 50 (c)	Engine Control System Failures
CS-E 1030	Time Limited Dispatch (Issue 1)

2.2 Acronyms and Symbols

AFM	Airplane Flight Manual
ARP	Aerospace Recommended Practice
CAA	Civil Aviation Authority (FAA of United Kingdom)
CFR	Code of Federal Regulations (a.k.a. FARs)
CPU	Central Processor Unit

CMR	Certification Maintenance Requirement
CS	Certification Specification (EASA nomenclature)
DDG	Dispatch Deviation Guide
EASA	European Aviation Safety Authority
EEC	Electronic Engine Control
EPR	Engine Pressure Ratio
FAA	Federal Aviation Administration (or Authority)
FL	Flight Length (in hours)
FADEC	Full Authority Digital Engine Control
FAR	Federal Aviation Requirement
HM (or HMC or HMU)	Hydromechanical (control or unit)
IFSD (or IFSDs)	In-Flight Shut Down(s)
IM	Installation Manual
JAA	Joint Airworthiness Authorities (of Europe) (replaced by EASA)
JAR	Joint Airworthiness Requirement (replaced by EASA CS publications)
LOTC	Loss of Thrust Control
LOPC	Loss of Power Control
LT	Long Time Fault/Fault State/Repair Interval
MEL	Minimum Equipment List (operator constructed, based on the MMEL)
MM (or MMs)	Markov Model(s)
MMEL	Master Minimum Equipment List (provided by aircraft manufacturer)
MPD	Maintenance Planning Document
MRB	Maintenance Review Board
ND	Non-Dispatchable Fault/Condition
OEM	Original Equipment Manufacturer
OSD	Operational Suitability Data
ST	Short Time Fault/Fault State/Repair Interval
TLA	Thrust Lever Angle
TLD	Time Limited Dispatch
TWA	Time Weighted Average (see Section 7)

λ	failure rate (failures per million hours)
μ	repair rate, given on a per hour basis
=	equals
$\approx$	approximately equal to
$\equiv$	defined as
$\geq$	greater than or equal to
$\leq$	less than or equal to
P	probability
T	time
t	time

3. APPLICABILITY

The applicability of these guidelines is primarily intended for FADEC-equipped engines certifying to 14 CFR Part 33, CS-E regulations, and the application of those engines to aircraft certifying under 14 CFR Part 23, 25, 27, and 29 regulations. For the purposes of this document, a reference to Part 25 should also be read as a reference to Part 23/Part 27/Part 29, for the TLD analysis. The approaches contained herein have been accepted in previous FADEC system approvals for engines installed on aircraft certified under 14 CFR Part 25 regulations. The continued acceptability of these approaches should be coordinated with the appropriate certification agency during any new certification effort. In addition, changes have been made to extend the applicability of the techniques across both the engine and aircraft certification authorities, to include CM-MMEL-001 Issue 1 Engine Time Limited Dispatch and Master Minimum Equipment List (MMEL).

This approach may also be applied to systems which are not FADEC systems.

4. HISTORICAL PERSPECTIVE

The concept of time limited dispatch (TLD) originated during the development and certification of FADEC systems used on the turbine (jet) engines of the Boeing 767 airplane. A brief discussion of some of the early applications of electronics to turbine engine controls is given in Appendix A.

5. INTEGRITY GUIDELINES

Improved dispatchability for the FADEC engine control systems was a major objective during the design and development of the Boeing 767 airplane. The approach pursued was to have the engine manufacturers conduct an analysis of all control system faults, which would include all electrical/electronic and hydromechanical/mechanical faults, to determine their influence on control system integrity. This analysis would determine the length of time a fault (or faults) could be allowed to exist - after which repair would be required - to achieve a given level of integrity. Early discussions with Seattle's Northwest Mountain (ANM) Region FAA office, which certified the 767 aircraft; New England's (ANE) FAA office, which certifies the Pratt & Whitney and General Electric engines; Britain's Civil Aviation Authority (CAA) office, which certifies Rolls-Royce engines; and all engine manufacturers ensued. Representatives from the FAA field operations office (Part 121) attended the above meetings also. Although not directly involved in certification matters, the FAA Part 121 group approves airline maintenance and operations policies and procedures, and their concurrence with the proposed approach was needed. For the purposes of this document, a reference to LOTC should be read as a reference to LOTC/LOPC for the TLD analysis. The discussions defined an LOTC event and established some significant integrity requirements for FADEC systems. The integrity requirements are contained in the recently issued revision to FAA Engine and Propeller Directorate policy letter on Time Limited Dispatch. For engines intended for Part 25 applications, the LOTC definition and the integrity requirements are as follows:

An LOTC/LOPC is defined in AC33.28-3, AMC 20-3A, and CS E-1030.

For applicants complying with CS E1030, it provides criteria in addition to LOTC criterion, among which:

- Failures leading to an inability to relight in flight shall be classified No Dispatch
- Failures leading to be one failure away from an Engine Hazardous Event shall be classified No Dispatch

When complying with CS-E 1030 and FAA policy, additional criteria may be considered in TLD analysis.

1. The average integrity of the control system has to be better than or equal to 100000 hours for faults that result in an LOTC event. In other words, the Fleet Average LOTC rate of the FADEC system has to be less than or equal to 10×10^{-6} failures per hour. This fleet average is to include all modes of control system operation, and, by definition, is the average of all dispatches, including full-up system dispatches. It should be noted that the LOTC rate objective may be different from 10×10^{-6} /EFH; CS-E 50 (c) (1) specifies that it has to be consistent with the safety objective associated with the intended aircraft application.
2. The engine control system is considered to be NOT dispatchable if the instantaneous LOTC rate is greater than 100×10^{-6} failures per hour. The instantaneous LOTC rate is defined as the calculated LOTC rate of a specific combination of failures at dispatch.
3. The control system should have a more restricted (i.e., short time) dispatch period if it has suffered a significant loss in redundancy or its instantaneous LOTC rate is between 75×10^{-6} and 100×10^{-6} failures per hour. The engine manufacturer may choose to place other dispatchable failures, which have an associated instantaneous LOTC rate less than 75×10^{-6} events per hour, in this short time dispatch category as well, as that would be conservative. (Dispatches in these configurations are generally handled via the aircraft's Master Minimum Equipment List (MMEL.) See Appendix D.)
4. A longer, but still restricted, dispatch interval is allowable when the instantaneous LOTC rate is less than 75×10^{-6} , but greater than the 10×10^{-6} , failures per hour overall target.

It has been generally accepted that if (1) the FADEC installations have been shown to comply with FAR 25.903(b) in the system configurations approved for TLD, and (2) approved TLD methods are used to monitor and govern maintenance of each engine's FADEC system, then the engines may be considered independent of each other when determining dispatch in service. Thus, the airplane could be dispatched with faults present in more than one engine's FADEC system. Since this last item involves application of TLD to the aircraft, the acceptability of this item is at the discretion of the aircraft certification authority.

The initial 10 per million hour LOTC rate integrity requirement for engines intended for Part 25 applications is documented in the revised advisory circular (AC) for FAR 33.28, AC 33.28 (or equivalent EASA AMC 20-3). An analysis to show that the control system is designed to meet this integrity requirement is usually submitted as part of engine certification. This is normally required - even when the applicant is not applying for TLD operations.

A remaining integrity requirement for aircraft certification is to show compliance with FAR(CS) 25.1309. This FAR relates to Systems and Equipment, and the requirement is that the probability of having a catastrophic multi-engine thrust loss event due to independent control system causes must be less than 10^{-9} failures on a "per hour of flight basis." In previous certifications, the FAA, EASA, and other certification authorities have agreed that the use of a fleet-wide average, control system caused LOTC rate, is acceptable when showing compliance with this requirement. Using a fleet wide LOTC rate for engine certification of 10×10^{-6} per hour results in compliance with the FAR/CS 25.1309 requirement for multi-engine aircraft. This is discussed in more detail for a twin-engine aircraft in 8.1. Thus, the integrity requirements for engine certification are consistent with those that come from aircraft certification with regard to the application of FAR 25.1309. (Note that single engine aircraft used in commercial service do not certify under Part 25 regulations; thus, FAR 25.1309 requirements do not apply to single engine aircraft.) For a twin engine aircraft, the specific risks for dual engine LOTC events, caused by loss of both engines' control systems due to faults, is given in 8.2 for the various dispatch configurations currently allowed in service. The acceptability of all dispatch configurations needs approval from the aircraft certifying authority as well. Hence, any new aircraft certification application requires coordination with the appropriate aircraft certifying authority to establish the aircraft level allowable dispatch configurations and the acceptability of the associated specific risks for limited time periods requested.

There was no intent to circumvent or establish a more severe requirement for FADEC system integrity during engine certification under 14 CFR Part 33 than would come from the aircraft certification under 14 CFR Part 25, FAR 25.1309, when the integrity requirements for FADEC systems were being established. The intent was merely to require that FADEC system integrity be equivalent to the established reliability of the then current hydromechanical engine control systems. For aircraft certifying under 14 CFR Part 25, FAR 25.901(b)(2) requires the engine control to be reliable between "normal inspections and overhauls." The above engine control system integrity requirements were considered to meet this requirement as well as the fail-safe requirements of FAR 25.901(c) and 25.1309(b). For Part 25 applications, TLD is a useful tool for assuring that appropriate instructions for continued airworthiness are provided, as required by FAR 25.1529.

It is interesting to note that since the issue of the original ARP5107 in June, 1997, there have been significant changes in engine-run reliability as a result of Extended-range Twin-engined Operations (ETOPS). In the newly coordinated activity on ETOPS requirements, the overall engine - including those IFSDs caused by aircraft systems, have to show an IFSD rate of 0.02 per 1000 hours to be allowed ETOPS operations with diversions of 3 hours or less, and an IFSD rate of less than 0.01 per 1000 hours for ETOPS operations with diversions of more than 247 minutes. Because of this, the allowance (by the engine manufacturer) for engine control system caused IFSDs has continued to be dramatically reduced. This reduction has not been the result of more restrictive FAA regulations with respect to engine control system caused IFSDs, but rather, the "pressure of ETOPS" IFSD events. Hence, the average overall FAA LOTC rate for transport aircraft engines continues to be limited to 10 events per 10^6 flight hours, although the engine manufacturer would not allow such a high rate (for just the control system) in ETOPS operations. Such an allowance would have too high an impact on the IFSD rate.

6. GENERAL ANALYSIS APPROACH

The general approach is to construct a model of the FADEC system which allows the integrity of the system to be analyzed in its full-up as well as the various fault configurations considered allowable for dispatch, and to "time average" those various states of operation to achieve the required average integrity. The integrity requirements defined by PS-ANE100-2001-1993-33.28TLD-R1, Policy for Time Limited Dispatch (TLD) of Engines Fitted with Full Authority Digital Engine Controls (FADEC) Systems, are listed in Section 5.

In general, the analysis used to determine compliance with the requirements can be completed using any analysis tool(s), provided that the tools and methods used are acceptable to the certifying authority. Hence, it is important to have discussions with the appropriate certifying office concerning the capabilities and limitations of the analysis tools before commencing the actual analysis. Examples of previous tools used include standard fault tree computer programs and Markov models.

The general rule for faults relating to a TLD analysis is this: if they affect the LOTC rate, include them in the analysis; if they do not affect the LOTC rate, leave them out. Obviously, a fault does not have to have an immediate effect on the operation of the engine to be included in the analysis. It is sufficient that the "instantaneous LOTC rate" of the control be influenced for the fault to be included in the analysis. A more detailed discussion of some typical FADEC system faults, and whether they should be included in the LOTC analysis, is given in Appendix C.

This document addresses the two types of TLD maintenance approaches as discussed in Section 14 of FAA policy PS-ANE100-2001-1993-33.28TLD-R1; the MMEL and Periodic Inspection/Repair Maintenance Approach. The MMEL maintenance approach is generally termed "on condition" or "time since fault," where the time at which the fault occurs is known, and the fault is repaired within a defined time limit of its occurrence. The Periodic Inspection/Repair approach involves a "scheduled inspection and repair" of the faults. The time of occurrence of the fault is not known, but rather, a periodic inspection for faults is made, and should a fault be found, it must be repaired at that time or within a defined time limit of the inspection.

6.1 FADEC System Configuration

The FADEC System is a hardware/software system which controls, monitors, and reports on the operation of the power plant. The FADEC System consists of the Electronic Engine Control (EEC), its associated software, all hardware with which the EEC communicates (including, but not limited to: fuel metering unit, actuators, actively controlled valves, sensors, ignition exciters, throttle, thrust reversers, health monitoring), and the communication channels utilized by the EEC (e.g., wire harnesses, pressure sense lines).

A typical (simplified) FADEC system configuration is shown in Figure 1. For simplification purposes, it is assumed throughout this report that all electrical/electronic elements of the control have redundant elements, that the redundant elements are identical, and that the control alternates between use of the redundant elements on each engine start. This last item minimizes the exposure time for the existence of latent faults in the electrical/electronic elements. The above assumptions need not be the case for the use of these guidelines, but essentially all the equations used herein would need modification to account for dissimilar redundancy and not alternating electronic element/channel operation.

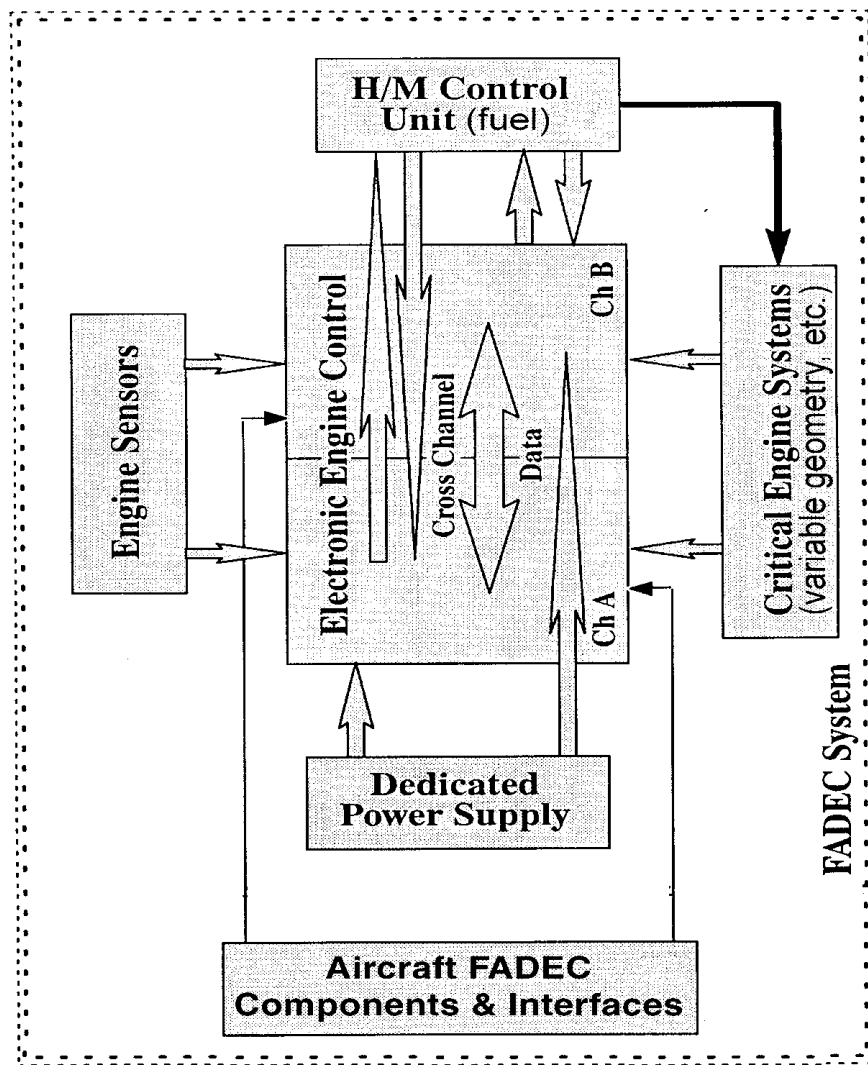


Figure 1 - Simplified FADEC system

6.2 Clarification and Management of Aircraft and Engine Control Faults Categories

Modern engine controls are increasingly reliant on airframe systems for critical inputs that may affect thrust control and dispatchability. Additionally, the control system may be providing data or functions that are utilized by airframe systems. These other systems (other than engine controls) may be a part of an MMEL for dispatch. When preparing a TLD report, in addition to identifying faults as Full Up Dispatch, Long Time Faults, Short Time Faults, and No Dispatch Faults, the applicant needs to clearly identify which faults are a function of the Engine or Engine Control and which faults are a function of another aircraft system. The faults that affect aircraft systems should be clearly identified in the engine TLD report. These faults could be included in or affect the aircraft level MMEL and be addressed by the airframer.

The original function of Full Authority Digital Engine Control (FADEC) system was to primarily manage the turbo machinery. Many of the functions are now incorporated in modern FADECs support aircraft functions. Section 6.5 provides elements to help the user to define the scope of the TLD analysis.

It is recommended that applicants clearly identify any functions that are not part of the Engine Control System in the TLD report. If these functions are to be included in the MMEL, they must be identified by the installer. This could be done as an appendix or addendum to the TLD report for clarity and ease of revision. The installation manual must include assumed airframe data reliability for the engine installation. Airframe data reliability should be considered while determining engine LOTC rate as described in 6.5.

6.3 Repair Categories: Immediate, Short, and Long Time

FADEC system faults can be grouped into one of three repair categories:

- Immediate or "no dispatch category" - As the name implies, faults in this category require repair prior to dispatch.
- Short time repair (or short time dispatch) - These faults are usually 500 hours or less, and dispatch decisions with these faults are typically handled via the aircraft Master Minimum Equipment List (MMEL). See Appendix D for further discussion of this item.
- Long repair interval (or long time dispatch) - These faults are typically 500 hours or more, and are typically handled via the operator's maintenance program.

The specific allocation of faults to the short or long time category is determined as part of "the conducting" of a TLD analysis. This determination can be influenced by an operator's maintenance policy.

The "Policy Letter from ANE FAA Regarding Time Limited Dispatch (TLD) for FADEC Controlled Engines," for TLD time limit restrictions applicable to "entry level" systems.

As indicated earlier, when complying with 14 CFR 2X.903 and showing that engine-to-engine isolation is maintained in all TLD approved dispatch configurations, it is not necessary to consider combinations of faults involving multiple engines when determining aircraft dispatch. If both the airplane and engine manufacturer wish to place limitations on TLD operations, the more restrictive of the two, on an item by item basis, should be used. For example, if the engine manufacturer indicates in the Instructions for Continued Airworthiness (ICA) for the engine that short time faults must be limited to 150 flight hours and long time faults should be limited to 500 hours, and the aircraft manufacturer places the limitation on the aircraft that short time faults should be limited to 100 flight hours and long time fault limited to 750 flight hours, the limitation should be 100 flight hours for short time faults and 500 hours for long time faults, as this is the more restrictive for each of the categories.

It is important to note that these repair categories are applicable to single faults as well as combinations of faults. For example, a mechanical/hydraulic fault that may not have caused an LOTC event on the last flight might be a stability bleed valve failure, where the bleed valve failed open, but did not cause EGT to increase to a level which would cause the flight crew to have to reduce thrust. Although the condition did not cause an LOTC event on the last flight, this is a single fault that requires immediate repair. (This assumes that the flight crew notes the effects of the failure condition and maintenance investigates and discovers the faulty condition.)

An example of a dual electronic fault that would normally require immediate repair is the loss of both channels' (free stream) total temperature sensors. This condition may not have resulted in a LOTC event on the last flight either, because the control may have been configured to accommodate such a fault. But it may be considered a non-dispatchable configuration for the control; hence, immediate repair may be required. Immediate repair is required for all combinations of faults that leave the FADEC system in a configuration where the instantaneous LOTC rate is greater than 100×10^{-06} failures per hour and/or all combinations of faults that leave the FADEC system within one fault away from LOTC.

A similar situation exists for the short and long time repair categories. A single fault, such as loss of the central processor in one channel, is a fault that is generally placed in the short time (i.e., less than 500 hours) repair category because the system suffers a significant loss of redundancy when such a fault occurs. The short time repair category might also be used to repair a condition caused by a combination of faults. For example, assume that the control experiences two independent faults, one in either channel, which by themselves might be placed in the long time (i.e., greater than 500 hours) repair category. The FADEC system could be configured so that when the two faults exist together, the repair requirement is "elevated" to the short time repair interval. This is required if the combination of faults results in a FADEC configuration where the instantaneous LOTC rate is greater than 75×10^{-06} failures per hour, but less than 100×10^{-06} failures per hour no-dispatch rate.

If two or more faults do not result in a condition of significance or concern, and by themselves, each would only require long term repair, then their combination may be left in the long time repair category as well.

Hence, in summary, the immediate (i.e., no dispatch), short time and long time repair categories can be used for single as well as combinations or multiple faults. The selection of the category is dependent on the condition of the control when operating with the fault(s).

As always, discussions between the appropriate authorities and aircraft OEMs should be held to confirm the acceptability of the various dispatch configurations and their respective operating intervals.

6.4 Classification of FADEC Fault Types

The approach used herein is to take all FADEC system faults, one by one, and determine which repair category is suitable for that fault, assuming that it is the only fault in the system, and that ultimately the fleet average LOTC rate of 10×10^{-6} failures per hour is achieved with the defined categorization. If the fleet average is not achieved, it will be necessary to place more restrictive dispatch limits on some of the faults to achieve the required rate.

6.4.1 No Dispatch (ND) Type Faults

Single faults that require immediate repair are termed no-dispatch (ND) type faults. (This should not be confused with combinations of faults that result in a no-dispatch condition.) The assumed FADEC system configuration (Figure 1) consists of redundant elements for all electronic/electrical portions of the system. Because of this assumed redundancy, the configuration has no known single electronic/electrical elements (from a functional perspective) which if failed, would require immediate repair to achieve a dispatchable configuration.

Note, however, that all single faults have to be assessed against the requirement that the instantaneous LOTC rate cannot be greater than 100×10^{-6} failures per hour when dispatching with the fault. If a single fault leaves the control in a configuration where the instantaneous LOTC rate is greater than this upper bound, the fault should be placed in the no-dispatch category. Exposure to these faults over a single flight are generally not included in the reliability analysis because the repair interval is so frequent, there is essentially no effect on the estimated LOTC rate.

Since the hydromechanical/mechanical elements of the system are assumed to be non-redundant, all ND type faults in the FADEC system discussed herein (Figure 1) are in the hydromechanical/mechanical elements. Only those ND faults which would lead to an LOTC event should be included in the analysis. If some fault redundancy is provided within the mechanical/hydromechanical elements, these can be treated as additional ST or LT faults provided the detectability and residual system reliability are adequate. The engine manufacturer(s) may elect to place single element items in the ND category that do not lead to an LOTC event. Examples of this might be an air-oil-cooler valve, which if failed open might result in the inability to maintain adequate fire extinguishing capability. Failure of such a valve would not generally lead to an in-flight LOTC event; therefore, these type ND faults should not be included in the TLD analysis.

6.4.2 Short Time (ST) Type Faults

Faults placed in the short time repair category (e.g., less than 500 hours) are termed ST type faults. From the requirements of Section 5, single faults which leave the control in an acceptable dispatch configuration, but one where the instantaneous LOTC rate is between 75×10^{-6} failures per hour and 100×10^{-6} failures per hour should be placed in this category. In addition, FAA approved TLD operations to date have all single faults which leave the control in essentially single channel operation, such as loss of one channel's CPU or power supply, placed in the ST category - even though the LOTC rate of the remaining channel may be less than 75×10^{-6} . Again, it is assumed that there are no single electrical/electronic faults which leave the control in a configuration where the instantaneous LOTC rate is greater than 100×10^{-6} failures per hour. If this were the case, those faults would have to be placed in the ND category. There are many applications where faults that could be placed in the long time category (discussed below) are placed in the Short Time category. Obviously, this is always acceptable.

6.4.3 Long Time (LT) Type Faults

Single faults placed in the long time (e.g., longer than 500 hours) repair category are termed LT type faults. Based on the requirements given in Section 5, LT faults must not leave the FADEC system in a configuration where the instantaneous LOTC rate is greater than 75×10^{-06} failures per hour. Examples of these faults might be loss of a sensor or any other input or feedback signal for which there is redundancy (or adequate fault accommodation in the case where redundancy is not provided for all electronic elements) - and a suitably low LOTC rate is maintained.

6.4.4 “Applicant Defined Dispatch” or “Engine Manufacturer/Airframer Convenience”

AMC E 1030 and FAA TLD policy memo, introduce a category for failure out of LOTC criteria.

This Engine Control System failures are classified in dispatch category “Applicant Defined Dispatch” (AMC E 1030) or “Engine Manufacturer/Airframer Convenience” (FAA TLD policy memo). These failures have to be assessed for TLD with engineering judgment or with Aircraft MMEL policy when these ones are included in HAZ or CAT Failure conditions as per CS 25.1309.

As prescribed by EASA CM MMEL 001 issued January 21, 2015, the dispatch on these failures must be in a separate section of TLD analysis and are not in TLD approval.

6.4.5 Combinations of Faults and Undetected (UC) Faults

Figure 2 shows a very simplified FADEC system fault configuration diagram which is used for the LOTC analysis. Figure 3A shows Figure 2 expanded into a flow diagram leading to the LOTC state. “Undetected faults” have been added to these diagrams. Undetected faults are faults in the electronic portions of each control channel for which no means of detection or accommodation has been provided. Since these faults are unaccommodated, it is assumed that they would lead to LOTC events. Typical undetected fault rates are between 0% and 5% of the total of both channels (electronic) failure rates. The analysis should provide substantiation for the value used. (It is noted that undetected faults which result in an LOTC event do not remain “undetected” for long. Some prefer classifying these as simply “uncovered” faults.)

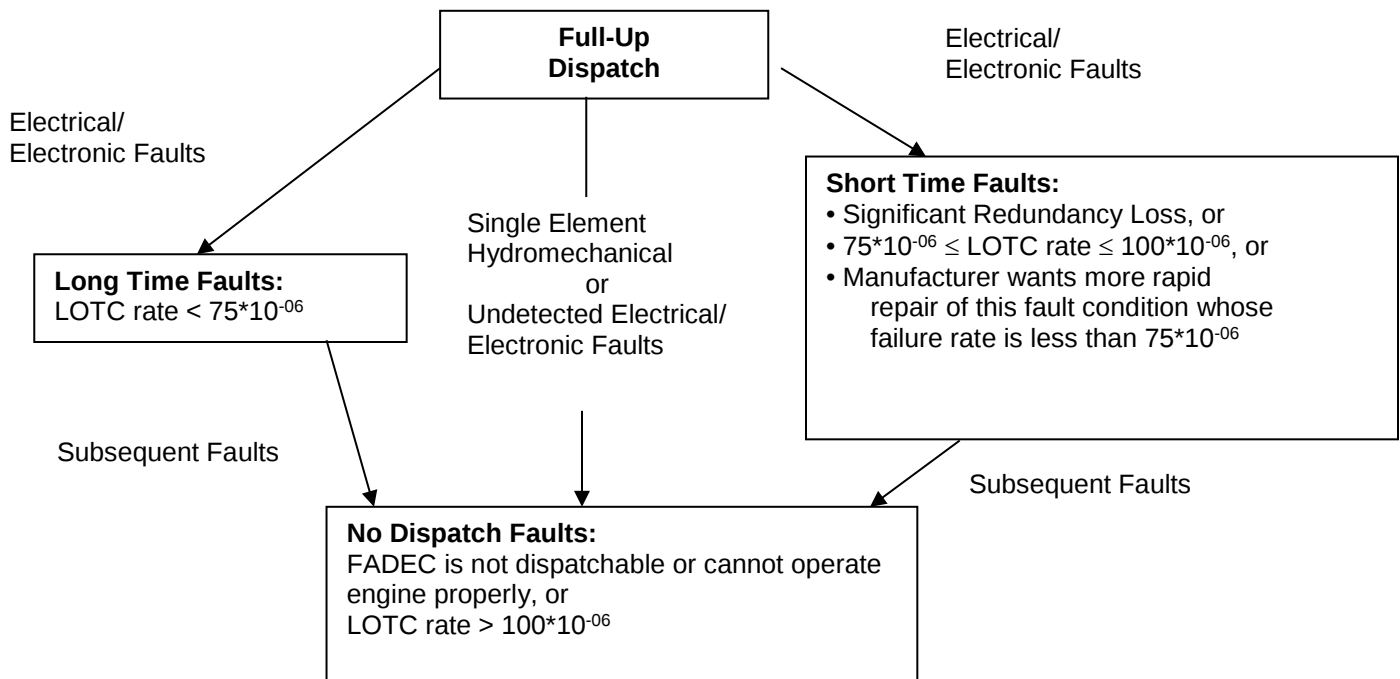


Figure 2 - Simplified FADEC system fault diagram

Figure 3A is not intending to imply that all combinations of ST and LT faults in both channels lead to LOTC events. The analysis has to look at each combination and determine whether they are truly independent and together would lead to an LOTC event. This is the cornerstone of any reliability analysis. The usage of the TLD approach is dependent upon the knowledge that the system has been thoroughly and accurately analyzed for operation with single and combinations of faults - at least to the second fault level. The third fault level does not have to be analyzed if the applicant elects to take the conservative position that all third faults lead to an LOTC event. The analysis will yield the conservative result that the repair intervals will be sooner than those that would have been obtained had third faults been analyzed. Analyzing the combinations of faults is the difficult and tedious part of the analysis, and this is where much of the work is. It should be noted if the analysis is only completed to the second fault level, there will be occasions in service when the FADEC systems are actually dispatched and operated with more than two faults present. However, the likelihood of three or more independent faults occurring within the short or long term repair interval - and still having the control function with no discernible effect - is quite small; therefore, the impact on the fleet average is expected to be negligible. A TLD analysis should include some analysis and documentation to substantiate this assertion.

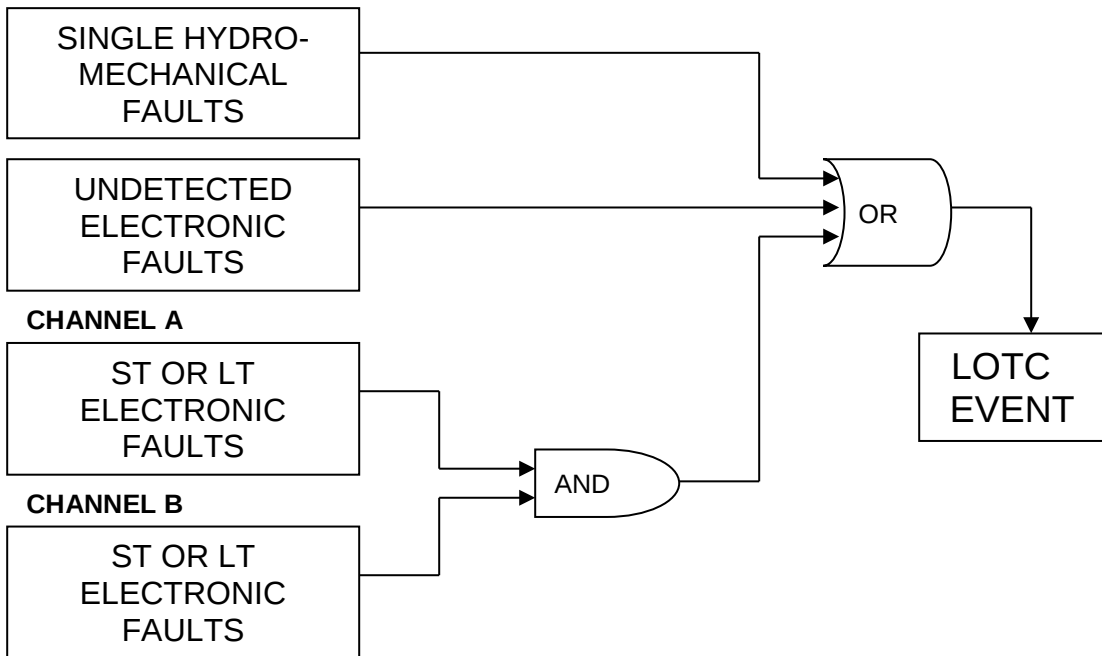


Figure 3A - Simplified flow diagram for FADEC system faults leading to LOTC

6.4.6 Aircraft Related Information

A discussion of the aircraft's MMEL, operator's MEL, dispatch deviation guide (DDG), and maintenance review board (MRB) report; how ND-, ST-, and LT-type faults relate to those documents; how LT faults became a certification maintenance requirement (CMR); and some options for handling LT faults to remove them from the CMR classification is presented in Appendix D.

6.5 Recommendations on Items Considered Part of the FADEC System

The question "What elements of the system are to be included?" is frequently raised relative to LOTC analysis and Time Limited Dispatch. This section addresses that question. The functions of the system, the elements selected for use in the system, and the design implementation all depend on the overall system architecture. In addition, integration between the engine and the aircraft control systems is constantly changing. All of these factors impact the selection of the elements to include as part of the FADEC system. Therefore, the information included in this section does not provide an absolute answer, but is intended to provide a methodology to use in selecting which elements of the aircraft/engine control system should be included in the analysis.

In general, the analysis used to predict the frequency of an LOTC should include all elements in the thrust or power control system that can contribute to an LOTC event. It is the overall LOTC rate for a given engine and aircraft that is relevant to obtaining and maintaining TLD in service.

Since TLD is a benefit to engine manufacturer customers, the engine manufacturer has a vested interest in obtaining TLD for the installed engine control system. Including the required aircraft elements in the analysis allows the engine certification authority visibility of total LOTC rates. Therefore, the engine manufacturers must include the relevant aircraft supplied control elements as part of the engine control system when seeking approval of TLD operations. The engine manufacturer may provide the airframe information by obtaining it from the airframer or by using data from the engine manufacturer's applicable prior history. The overall installed engine LOTC rates will also be reviewed and used by the aircraft certification agency in approving TLD operations for the aircraft.

Note that the LOTC analysis and reporting does not include the details, analysis, and corrective actions associated with basic engine events. And the engine manufacturer is not expected to (1) substantiate any airframer predictions, (2) explain the details of aircraft element failures which contribute to LOTC events, or (3) monitor and manage any resulting changes to the aircraft systems. Hence, the engine manufacturer may not be in a position to provide detailed information on any aircraft element failures which could lead/contribute to LOTC events, even though those aircraft elements are considered part of the engine control system. It is anticipated that when LOTC events occur, the engine manufacturer will be made aware of them. If those events are caused by aircraft elements which are part of the engine control system, the engine manufacturer is expected to coordinate with the aircraft manufacturer to determine whether corrective actions are needed - so that the engine control system can continue to meet its Continued Airworthiness requirements.

In general, the following guidelines apply when selecting the elements to include in the LOTC analysis:

- The LOTC event is related to an engine control failure or malfunction. The engine control system failure may involve aircraft supplied element failures or malfunctions. In some cases, the failure may result in flight crew action to reduce power or thrust, or initiate an engine shutdown.
- All In-Flight Shut Downs (IFSDs) are a subset of LOTC events (see Figure 3B), and all engine control system caused or induced IFSDs and fail fixed rotor speed, thrust or fixed fuel flow conditions are forms of LOTC.
- If a component is part of the control system and its failure or malfunction can contribute to an LOTC event, it should be included in the LOTC analysis.
- If a component is not directly part of the engine control system but has an electrical interface with the EEC, it is a candidate for contributing to an LOTC event and should be considered for inclusion in the analysis.
- If a component is part of the basic engine mechanical system, but not part of the mechanical portion of the engine control system, it is usually not a candidate for an engine control system related LOTC event, and therefore, not included in the engine control system LOTC analysis.
- The FAA TLD policy allows exclusion of the fuel pump from being included as part of the engine control.
- Components to be included are not limited to the redundant electrical parts of the control system.
- If a component can cause an erroneous value to be displayed in the cockpit, and the Installation and Operational Manuals published by the engine manufacturer either direct or advise the crew to shut down the engine or reduce thrust or power, the component should be included in the LOTC analysis.
- LOTC events which directly result from a failure to follow instructions in the manuals published by the Engine Manufacturer are not included in the analysis.
- LOTC events which do not occur during normal operation (operations outside conditions defined in the engine IM or AFM) are not included in the TLD analysis.

Figure 3B attempts to illustrate the concept of selecting the events and causes of the events, and hence, the elements to be included in the TLD analysis.

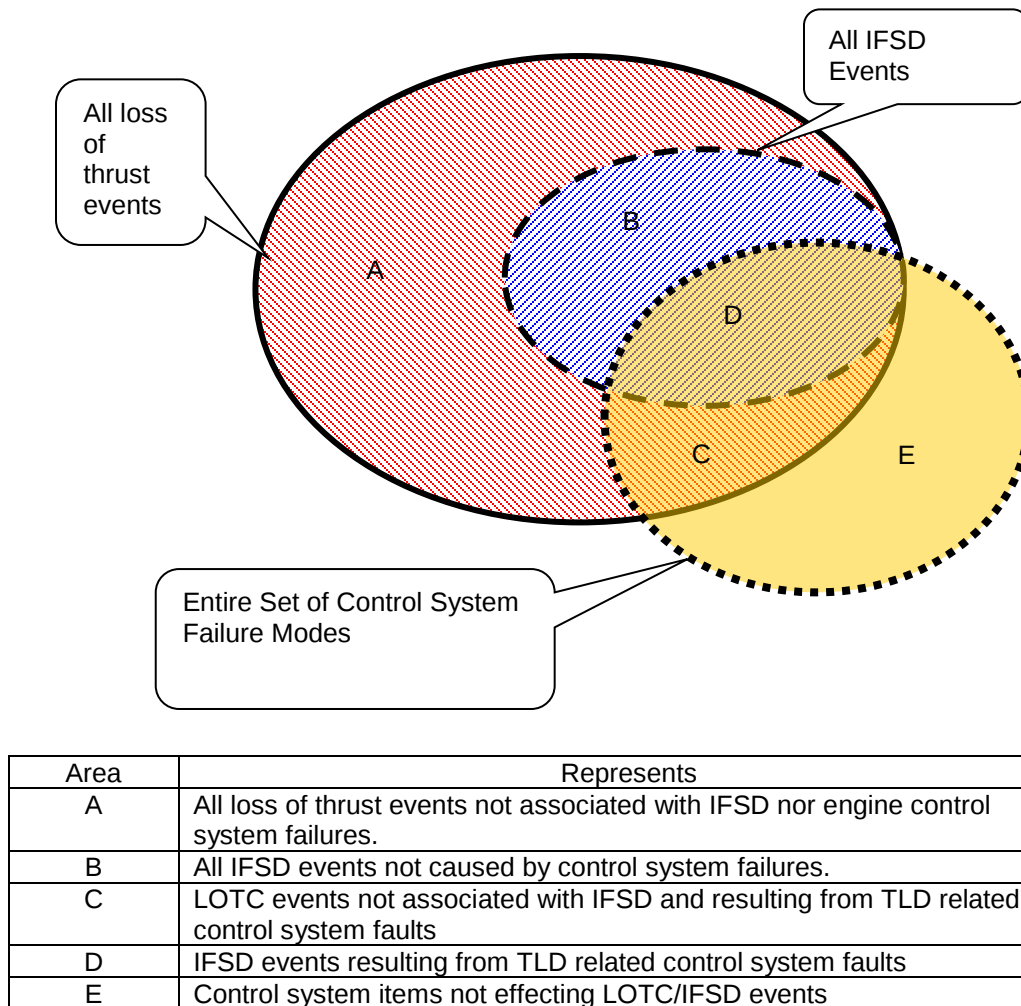


Figure 3B - Illustrations of all LOTIC events, all IFSD events, and engine control system elements involved in a TLD analysis

Figure 3

Figure 3B is intended to provide visibility on what power plant faults have to be taken into account in the TLD analysis. Specifically, LOTIC is a term referring to loss of thrust control events caused only by the Engine Control System.

The envelope shown as “Entire Set of Control System Failure Modes” includes some, but not all, LOTIC events and some, but not all, IFSD events. The subset of those events applicable to TLD that overlap the TLD considerations envelope are shown as areas “C” and “D.” Those LOTIC and IFSD events not applicable to TLD are shown as areas “A” and “B.”

As discussed in 6.3, there are many functions in an EEC system that have no effect on the LOTIC rate of the control. These items have to be given consideration as candidates when completing the task of “considering what items should be in the TLD analysis” to document the fact that they have no impact on the control system’s LOTIC rate. These items are represented by area “E” in Figure 3B. These EEC system functions faults that do not affect LOTIC rate should be clearly identified in the Engine TLD report. These faults could be included in or affect the aircraft level MMEL and be addressed by the airframer.

Table 1 illustrates how to consider all elements of the thrust or power control system, the functions and failure modes associated with the element, and then evaluate if it is or is not part of the TLD restriction envelope depicted in Figure 3B. The table also shows the most likely result of a failure of the element by identifying the applicable area of Figure 3B.

Table 1 - Typical categorization of FADEC system elements

Engine Electrical Control System			
<i>Item</i>	<i>To Be Included</i>	<i>Figure 3B Failure Area</i>	<i>Included Yes/No/If</i>
EEC	Primary engine control providing power setting, fuel flow setting and splitting, engine operability control, and engine limit protection functions.	C or D	Yes
	Auto or continuous ignition may need to be included.	C, D, or E	If
Engine Condition/Health Monitoring	Yes, if impact on LOTC rate.	C, D, or E	If
	No, if no impact on LOTC rate (inspection is presumed to provide adequate analysis).		
Other electronic boxes	Yes, if it has impact on LOTC rate. (If not, area "E.")	C, D, or E	If
	Yes, if it includes processing of signals listed elsewhere that affect LOTC rate. (Area "E" if no effect on LOTC rate.)	C, D, or E	
	Yes, if it includes processing of fault detection and reporting data related to TLD.	C or D	
Ambient temperature and pressure sensors	Yes, for FADEC dedicated sensors. (Unless the system is configured to use the aircraft sensors as primary or only.)	C (possible D)	Yes
Engine operating parameter sensors (pressure, temperature, speed)	Yes, sensors that may contribute to LOTC.	C	If
	No, sensors used only for monitoring; e.g., engine performance monitoring or secondary systems.	E	
Electrical cables, including airframe cables (as appropriate)	Yes, but only for cables that carry a signal applicable to LOTC/IFSD.	C	If
Igniters, ignition exciter, and associated cables	No.	N/A	No
Dedicated EEC alternator	Yes, includes the electrical generation portion of the alternator and any drive shafts/couplings/bearings within the alternator.	C or D	Yes
Alternator Drive Assembly (but not part of alternator)	No.	A or B	No
Cockpit throttle position elements	Yes, for electrical throttle position sensor and aircraft electrical cables connecting the sensor to the EEC.	C or D	Yes
	No, for mechanical parts of throttle system.	A or B	
Aircraft data bus inputs to EEC	Yes, if it can contribute to engine control system caused LOTC.	C	If
Rating, configuration, and thrust trim definition (connectors/boxes)	Yes, if it can contribute to LOTC rate.	C	Yes

Engine Electrical Control System			
<i>Item</i>	<i>To Be Included</i>	<i>Figure 3B Failure Area</i>	<i>Included Yes/No/If</i>
Engine fault detection sensors, conditioners, and computers (e.g., overspeed limiters)	Yes, if effect on LOTC rate and control system operation/maintenance. (Area "E" if no effect on LOTC rate.)	C, D, or E	If
Engine transient performance	Yes, if caused by failure within the control system. No, if caused by engine damage or deterioration preventing it from operating with correctly implemented control limits.	C A	If
Engine transient due to lightning strike	No, if events caused by engine damage due to direct effects or engine surges due to pressure/thermal inlet effects. Yes, if control system upsets caused by EMI, HIRF, or the indirect effects of lightning. This is true during all dispatchable configurations. Control related events must be reported.	A or B	If
Inappropriate pilot commanded shutdown	No	B	No
Aircraft auto throttle or auto thrust system	No	A	No

Fuel System			
<i>Item</i>	<i>Comments</i>	<i>Figure 3B Failure Zone</i>	<i>Included Yes/No/If</i>
Mechanical fuel pump	No, excluded per FAA policy. Considered part of basic engine.	A or B	No
Accessory gearbox elements associated with fuel pump or Metering Unit Drive	No, engine mechanical systems are not considered to be part of the control system.	A or B	No
Fuel Filter Condition sensors	Yes, if fault results in restriction on power setting or time at power.	C	If
Flow meter	Yes, if active part of fuel control.	C or D	If
Fuel metering unit	Yes.	C or D	Yes
Active fuel flow divider valves	Yes, assumes fault results in restriction on power setting or time at power. Active refers to any valves that are controlled by the FADEC to divide or stage flow to the burner.	C or D	Yes
Combustor flow control	Yes, assumes fault results in restriction on power setting or time at power.	C or D	Yes
Other fuel actuated control units	Yes, if unit associated with the control of any function listed elsewhere as applicable.	C or D	If
Fuel nozzles and fuel lines	No, considered part of basic engine.	A or B	No
Fuel temperature or pressure sensors	Yes, if the fault results in restriction on power setting or time at power.	C	If
Fuel lines, manifolds, etc.	No, considered part of basic engine. Fixed position flow distribution or pressure modification devices within the manifolds are included in the same category as fuel lines and manifolds.	A or B	No

Variable Geometry and Bleed Systems			
<i>Item</i>	<i>Comments</i>	<i>Figure 3B Failure Zone</i>	<i>Included Yes/No/If</i>
Compressor Variable Stator Vane Actuators and position sensors	Yes, assumes fault can impact engine performance to cause a LOTC. Actuator means the device that receives the air or fuel muscle to position the loop.	C or D	Yes
Variable (Bleed) actuators and position sensors	Yes, assumes fault can impact engine performance to cause a LOTC. Actuator means the device that receives the air or fuel muscle to position the loop.	C or D	Yes
Variable Stator Vane and Bleed Actuation System Unison Rings, links, clevis, vane bearings, etc.	No, defined as all mechanism(s) connecting the control actuator mechanical output to the variable position air flow device.	A or B	No
Air bleed valves (transient or start)	Yes, assumes fault results in reduction in power or a restriction on power setting or time at power.	C	Yes
Pneumatic and hydraulic servo lines used to provide force to position valves, actuators, etc.	Yes, tubes and hoses which provide pneumatic or hydraulic pressure used to position valves and actuators, assuming that mis-positioning of these valves or actuators could result in an LOTC.	C	Yes

Engine Oil/Lubrication System			
<i>Item</i>	<i>Comments</i>	<i>Figure 3B Failure Zone</i>	<i>Included Yes/No/If</i>
Oil tanks and lines	No.	B	No
Mechanical Oil Pumps	No.	B	No
Electronic Debris sensors and conditioners	No, assumes there is no control-initiated input to power setting.	N/A or E	No
Filter condition sensors	No, assumes there is no control-initiated input to power setting.	A, B, or E	No
Temperature and pressure sensors	Yes, if there is control-initiated input to power setting or if a control system fault leads to erroneous indication which the Engine Operating Instructions would require the pilot to reduce power.	C or D	If

Aircraft Interfaces			
<i>Item</i>	<i>Comments</i>	<i>Figure 3B Failure Zone)</i>	<i>Included Yes/No/If</i>
Vibrations sensors and conditioners	No, assumes there is no control-initiated input to power setting. Yes, if a control system fault leads to erroneous indication which the Engine Operating Instructions would require the pilot to reduce power.	A C or D	No If
Engine performance/ health monitoring sensors wired direct to cockpit	No.	A	No
Aircraft Power	Yes, if the failure of aircraft power can affect LOTC rate.	C or D	If

Propulsion System and Installation			
<i>Item</i>	<i>Comments</i>	<i>Figure 3B Failure Zone</i>	<i>Included Yes/No/If</i>
Basic engine turbo-machinery	No.	A or B	No
Engine Operability or Performance	No, includes thrust loss due to engine deterioration, surge, and reduction of power required to stay within limits. Yes, if a surge results in engine power fluctuations and that surge would have been prevented by a properly functioning control system, or was caused by an improperly functioning control system.	A or B	If
Thrust reverser position sensors	Yes, if a failure of a thrust reverser position sensor can result in a change in thrust setting (e.g., selection of idle thrust).	C	If
Thrust reverser actuation and control systems	No, if fault results in inability to deploy or stow the reverser but does not restrict engine power setting. Yes, if the engine does not provide commanded thrust.	N/A C	No Yes
Engine anti-icing sensors, controllers, and control valves	Yes, if these elements are used within the engine control system for automatic engine internal anti-icing.	C	If

Propulsion System & Installation			
<i>Item</i>	<i>Comments</i>	<i>Figure 3B Failure Zone</i>	<i>Included Yes/No/If</i>
Sensors, cables, or signal processing elements for aircraft electric or hydraulic power	No	A	No
Cockpit display signals	Yes, if erroneous display can lead to flight crew initiated thrust reduction or IFSD; e.g., incorrect rotor speed or EGT displayed. No, if only informational (e.g., fuel flow).	C or D E	If
Cockpit Display Systems	No, cockpit display systems are not considered part of the engine control system.	A or B	No
Aircraft Bleed Extraction	No.	A	No

Engine Configuration			
<i>Item</i>	<i>Comments</i>	<i>Figure 3B Failure Zone</i>	<i>Included Yes/No/If</i>
Brackets/clamps mounting bolts, seals, etc. associated with elements listed as applicable	No.	N/A	No
Thermal shields and insulation blankets	No.	A or B	No

Engine Configuration			
<i>Item</i>	<i>Comments</i>	<i>Figure 3B Failure Zone</i>	<i>Included Yes/No/If</i>
Pneumatic lines to sensors	Yes, if fault detection and accommodations can result in an LOTC.	C or D	Yes
Powerplant sensors which communicate directly with the aircraft and do not communicate with the EEC	No.	B	No

Items Unique to General Aviation Applications or Rotorcraft			
<i>Item</i>	<i>Comments</i>	<i>Figure 3B Failure Zone</i>	<i>Included Yes/No/If</i>
Collective Compensation Input	Yes, for electrical compensation sensor and associated electrical cables.	C	Yes
	No, for mechanical parts of the compensation system.	N/A	No
FADEC back up battery	Yes.	C or D	Yes
Torque Sensor	Yes, if the system has torque control or limiting.	C	If
Turbine temperature sensing system	Yes, if system has temperature limiting or OEI limiting, or pilot reduces power due to false (high) indication.	C	If

6.6 Recommendations on In-Service LOTC Reporting

After TLD approval is obtained and field experience is achieved, the FAA policy requires reporting of the field experience to provide continuing validation of the TLD analysis, identification of emerging trends that require field action, component redesign, etc. As part of this reporting process, the engine manufacturer should collect the data for all LOTCs that occur on an installation, including any that are caused by aircraft systems.

Only actual LOTC events shall be counted for reporting relative to the allowable event numbers provided in the FAA policy. Some failures occur without an LOTC that are identified by system fault detection. Corrective action is taken before an LOTC event has occurred. If those same failures had occurred at a different engine operating condition, an LOTC may have occurred. Since there was no LOTC, none is reported against the allowable number of events criteria. However, the TLD analysis related to these failures should be reviewed to determine if appropriate failure rates for the failures was used in the analysis. Even though it may not have caused an LOTC event, if the failure rate for the in-service faults and their effect on the LOTC rate is considerably greater than the one used in the TLD analysis, corrective action should be considered. Corrective actions may involve a greater restriction on the time allowed for operating with faults that contribute to the failure mode of concern, or redesign and replacement of the parts involved to achieve the desired design reliability for those components.

7. CALCULATION APPROACHES - SINGLE ENGINE ANALYSIS

7.1 A Simple Time-Averaging Approach

Note that the terminology "fleet average" is used synonymously with "time-weighted average." This is appropriate because any given engine may have more or less ST and/or LT faults than the expected number, but these guidelines are intended for use in a large fleet of engines where all possible single faults will occur at or close to their expected rates, and if all faults are allowed to remain in the system for the maximum approved number of hours before repair is accomplished, the LOTC rate of the control will approach the expected value. It is recognized that in practice, many faults are repaired sooner than the maximum allowed time; therefore, the fleet averaged LOTC rate may be quite a bit lower than the expected value.

A simple "time-weighted-averaged (TWA) LOTC rate" is one wherein the LOTC rate is determined as the sum of (1) the hydromechanical/mechanical failures, (2) the undetected faults, and (3) a time-weighted-average value of the FADEC system's dual channel, electrical/electronic failures. The failures and failure rates leading to an LOTC event are shown graphically in Figure 4.

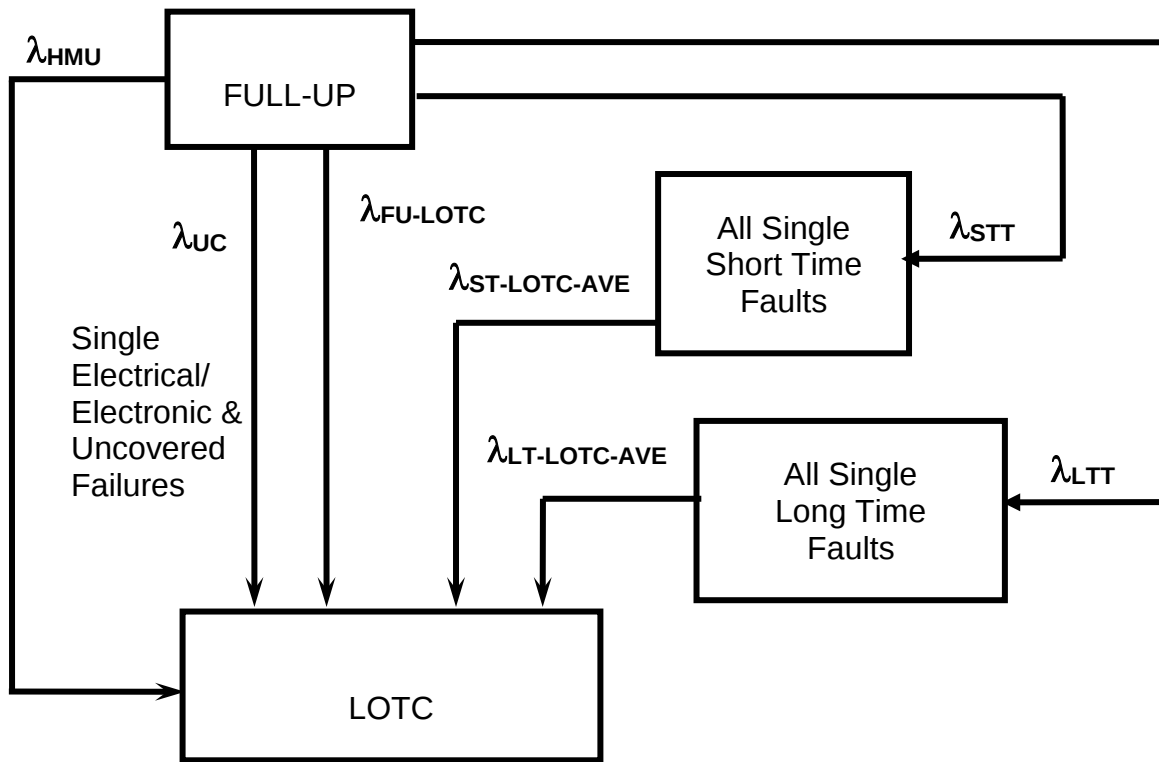


Figure 4 - A graphical representations of the failure paths of a simple FADEC system that lead to LOTC

The TWA failure rate for the dual channel electronic failures is determined as the sum of single hydromechanical and undetected electrical/electronic failures that lead directly to an LOTC event plus the percentages of time spent in a given operating configuration multiplied by the average LOTC rate of that configuration. Hence, the fleet TWA LOTC rate for a simple FADEC system is given as:

$$\lambda_{\text{LOTC-AVE}} = \lambda_{\text{HM+UC}} + \lambda_{\text{FU-LOTC}} * \text{Fract}(\text{FU}) + \lambda_{\text{ST-LOTC-AVE}} * \text{Fract}(\text{ST}) + \lambda_{\text{LT-LOTC-AVE}} * \text{Fract}(\text{LT}) \quad (\text{Eq. 1})$$

where: $\lambda_{\text{HM+UC}} = \lambda_{\text{HMC}} + \lambda_{\text{UC}}$

λ_{HMC} represents the sum of the rates of all single mechanical/hydromechanical faults which lead to LOTC events.

λ_{UC} represents the sum of the rates of all undetected/uncovered electrical/electronic faults assumed to lead to LOTC events.

$\lambda_{\text{FU-LOTC}}$ is the (average) failure rate from the full-up configuration to the LOTC state caused by failures in the redundant portions of the electronic control system, in one flight. (Single electrical/electronic failures that lead to an LOTC event are contained in λ_{UC} , which is described below.)

$\lambda_{\text{ST-LOTC-AVE}}$ is the average failure rate of the system due to a second electrical/electronic fault when operating in an ST fault dispatch configuration.

$\lambda_{\text{LT-LOTC-AVE}}$ is the average failure rate of the system due to a second electrical/electronic fault when operating in an LT fault dispatch configuration.

The undetected fault rate, λ_{UC} , is generally expressed as:

$$\lambda_{UC} = X * \{ \sum \lambda \text{ of both channel electrical/electronic faults associated with LOTC critical elements} \} \quad (\text{Eq. 2})$$

where:

The " $\sum \lambda$ of all electrical/electronic hardware associated with LOTC critical elements" can be approximated by $(\lambda_{STT} + \lambda_{LTT})$, where λ_{STT} is defined as the sum of the failure rates of all ST type faults in both channels, and λ_{LTT} is defined as the sum of the failure rates of all LT type faults in both channels. Hence,

$$\lambda_{STT} \equiv \sum (\lambda_{ST(i)}), \text{ the sum of the failure rates of all ST faults in both channels} \quad (\text{Eq. 3a})$$

where $\lambda_{ST(i)}$ represents the failure rate for a particular ST fault.

$$\lambda_{LTT} \equiv \sum (\lambda_{LT(i)}), \text{ the sum of the failure rates of all LT faults in both channels} \quad (\text{Eq. 3b})$$

where $\lambda_{LT(i)}$ represents the failure rate for a particular LT fault.

And "X" is a number generally between 0 and 0.05.

NOTE: Although Equation 2 might imply that the undetected fault rate is assessed at the "channel" level, in actual practice, it isn't. The undetected fault rate is usually determined by summing the undetected fault rates of all LOTC critical elements, on an element-by-element basis - such as the power supply, the CPU, sensors, A/D converters, etc. Equation 2 tends to imply that the undetected fault rate of each element is between 0 and 5%. This is not intended. Equation 2 is merely a simplification indicating that a channel's overall undetected fault rate will "generally" be somewhere between 0 and 5% of the channel's total LOTC rate.

Equation 2 is quite conservative because it assumes that an undetected fault in either channel would lead to an LOTC event - in any given flight. In practice, many different system architectures are possible, each of which utilize varying degrees of system resources and each with its own unique level of system coverage. For these systems, Equation 2 can be modified to provide a more accurate representation of the architecture. For example, assume that the system being addressed is an active-standby system, which is currently representative of many of the current designs. In these systems, the controlling channel provides all of the required resources when operating in a full-up condition. Furthermore, the alternating channel scheme (i.e., the process of alternating control channels on each engine start), provides nearly 100% coverage of undetected faults in the standby channel at the next engine start. Hence, an undetected fault in the standby channel in a given flight would not cause an LOTC event unless the operating channel has a fault (in that flight) which requires the system to "switch" channels. The likelihood of this is relatively small for most channel switching schemes. Hence, for these system configurations, the value of λ_{UC} may be reduced by approximately $\frac{1}{2}$ because the vast majority of undetected faults that lead to an LOTC event are only those in the active channel.

In any case, knowledge of the system configuration and its operating characteristics should be used when determining the value of the undetected fault "multiplier."

Continuing with Equation 1:

Fract(FU) is the fraction of time spent in the full-up state,

Fract(ST) is the fraction of time spent in the short time dispatch state,

Fract(LT) is the fraction of time spent in the long time dispatch state.

The following discussion uses the nomenclature "T" to represent repair times. This T repair time is the same time period that the system is allowed to operate with a given fault before repair is required.

Assume a block of time of a million hours. During the million-hour block of time, the system is in the full-up state for $\text{Fract(FU)} * 10^6$ hours, the system fails from the full-up state to the ST state at a rate of λ_{STT} per hour, and for each of those failures it remains in the ST state for $T_{ST\text{-REPAIR}}$ hours. Therefore, the fraction of the million hours spent in the ST state is:

$$\text{Fract(ST)} = \text{Fract(FU)} * (\lambda_{STT} * T_{ST\text{-REPAIR}}) \quad (\text{Eq. 4a})$$

And likewise, the fraction of time spent in the LT state is:

$$\text{Fract}(\text{LT}) = \text{Fract}(\text{FU}) * (\lambda_{\text{LTT}} * T_{\text{LT-REPAIR}}) \quad (\text{Eq. 4b})$$

Combining these equations with the conservation requirement that:

$$\text{Fract}(\text{FU}) + \text{Fract}(\text{ST}) + \text{Fract}(\text{LT}) = 1 \quad (\text{Eq. 5})$$

Leads to the fractions:

$$\text{Fract}(\text{FU}) = \frac{1}{1 + \lambda_{\text{STT}} * T_{\text{ST-REPAIR}} + \lambda_{\text{LTT}} * T_{\text{LT-REPAIR}}} \quad (\text{Eq. 6a})$$

$$\text{Fract}(\text{ST}) = \frac{\lambda_{\text{STT}} * T_{\text{ST-REPAIR}}}{1 + \lambda_{\text{STT}} * T_{\text{ST-REPAIR}} + \lambda_{\text{LTT}} * T_{\text{LT-REPAIR}}} \quad (\text{Eq. 6b})$$

$$\text{Fract}(\text{LT}) = \frac{\lambda_{\text{LTT}} * T_{\text{LT-REPAIR}}}{1 + \lambda_{\text{STT}} * T_{\text{ST-REPAIR}} + \lambda_{\text{LTT}} * T_{\text{LT-REPAIR}}} \quad (\text{Eq. 6c})$$

As discussed in 7.1.4 and 7.1.5, and shown in Figure 5, the use of these fractional coefficients provides a much-improved result as compared with the fractional coefficients as defined in the original release of this ARP. This is because the fractional coefficients defined by Equations 6 of this revised ARP adjust in a more balanced manner to reflect the actual portion of time spent in the various states. The definitions of the fractional coefficients in the original ARP did not do this because the Fract(ST) and Fract(LT) fractional coefficient terms, as developed in original ARP, assume the control is in the full-up state for the full million-hour block of time. In this revised ARP, it is recognized that the control is only in the full-up state for Fract(FU)*10⁶ hours.

7.1.1 LOTC Rate for Full-up Electronics

For small λT s, the LOTC rate for the full-up electrical/electronic portions of the control at dispatch is approximated as:

$$\lambda_{\text{FU-LOTC}} \leq [(\lambda_{\text{STT}} + \lambda_{\text{LTT}})/2]^2 * T_{\text{FL}} \quad (\text{Eq. 7})$$

where:

λ_{STT} and λ_{LTT} are defined above

T_{FL} represents the length of a flight (in hours)

This full-up channel failure rate is a very conservative estimate because it assumes that all channel faults (both short time and long time) result in loss of that channel. Although this is far from accurate, it surely provides an upper bound. The calculated value of $\lambda_{\text{FU-LOTC}}$ is usually quite small, as it should be. This is because it takes two independent, electrical/electronic failures, one in each channel, to have an LOTC event occur in one flight from the full-up configuration. The small value of $\lambda_{\text{FU-LOTC}}$ serves to show that the redundant electronic portions of the control have little effect on the LOTC rate of the control system when operating in the full-up configuration.

7.1.2 Average LOTC Rate for Short Time (ST) Faults

The certifying authorities have indicated that all faults which deplete a significant portion of the control system's capability should be repaired in a short period of time. Hence, sum the failure rates of the power supply and processor unit elements of both channels, along with any other items that are deemed necessary of requiring short term maintenance, and set the repair interval for these elements equal to (or slightly greater than) the maximum MEL dispatch deviation time allowed in the application.

An average LOTC rate for operation with one of these faults is useful. Grouping the above faults together as ST repair faults, the "average" LOTC rate with a short time (ST) fault is defined as follows:

$$\lambda_{ST-LOTC-AVE} = \frac{\sum\{\lambda_{ST(i)} * \lambda_{LT-LOTC(i)}\}}{\sum\{\lambda_{ST(i)}\}} \quad (\text{Eq. 8})$$

where:

$\lambda_{ST(i)}$ is the failure rate for a given ST fault, and $\lambda_{LT-LOTC(i)}$ is the failure rate to the LOTC state when operating with that particular $\lambda_{ST(i)}$ fault. (Include all faults in the 'other' channel that would lead to an LOTC event, but do not include the hydromechanical and undetected faults, as they are already accounted.)

7.1.3 Average LOTC Rate for Long Time (LT) Faults

Excepting the "no dispatch" and "short time" faults, group all remaining electrical/electronic faults affecting LOTC of one channel together and place them in the long time repair category. As in the above discussion, an average LOTC rate is useful (for calculation purposes) for these long time faults. This is defined as:

$$\lambda_{LT-LOTC-AVE} = \frac{\sum\{\lambda_{LT(i)} * \lambda_{LT-LOTC(i)}\}}{\sum\{\lambda_{LT(i)}\}} \quad (\text{Eq. 9})$$

where:

$\lambda_{LT(i)}$ is the failure rate to a given LT fault state, and $\lambda_{LT-LOTC(i)}$ is the failure rate to the LOTC state when operating with that given $\lambda_{LT(i)}$ fault. (Again, include all faults of the 'other' channel and cross-talk link faults which would lead to an LOTC event, but do not include HMC or undetected faults.)

In general, many LT faults have only a minor effect on the control. For example, assume that one channel has a sensor failure, such as one of two actuator feedback position signals. The LOTC rate when operating with this signal would be the sum of the failure rates for (1) the redundant sensor, (2) the other channel's CPU and power supply sources and circuitry, and (3) the cross-talk link between the two channels. These are the only failures that would lead to an LOTC event, because these are the only paths that would cause loss of both actuator feedback signals to the control. (It is assumed in this example that an actuator feedback position signal is needed to maintain control of the engine. If controller logic is constructed to re-configure the control laws to work with no actuator position feedback information, this LT fault could well be deleted from the analysis.)

7.1.4 Calculations of the Average LOTC Rate Using the TWA Approach

Having summed all of the ST and LT faults rates to obtain λ_{STT} and λ_{LTT} ; and determined the average failure rates $\lambda_{ST-LOTC-AVE}$ and $\lambda_{LT-LOTC-AVE}$ from Equations 8 and 9, the average overall LOTC rate given by Equation 1 can be calculated.

Using the balanced fractional coefficients given in Equation 6 in Equation 1 yields the LOTC rate as:

$$\lambda_{LOTC-AVE} = \lambda_{HM+UC} + \frac{\lambda_{FU-LOTC} + (\lambda_{STT} * T_{ST-REPAIR}) * \lambda_{ST-LOTC-AVE} + (\lambda_{LTT} * T_{LT-REPAIR}) * \lambda_{LT-LOTC-AVE}}{\{1 + \lambda_{STT} * T_{ST-REPAIR} + \lambda_{LTT} * T_{LT-REPAIR}\}} \quad (\text{Eq. 11})$$

Using the above TWA equation, which used the balanced fractional coefficients of Equations 6 to estimate the average LOTC rate of the control system, yields a result which is considerably improved as compared with the fractional coefficients defined in the original release of this ARP. It is a more balanced approach because the fractional coefficients are more representative of the amount of time that is spent in each of the three states, i.e., full-up, short time fault (or dispatch), and long time fault (or dispatch). This is illustrated in the following example.

7.1.5 An Example Calculation

Assume the following data:

$$\lambda_{HMC} = 4.0 \times 10^{-6} \text{ (failures/hour)}$$

$$\lambda_{STT} = 30.0 \times 10^{-6} \text{ (failures/hour) (sum of ST electronic faults for both channels)}$$

$$\lambda_{LTT} = 70.0 \times 10^{-6} \text{ (failures/hour) (Sum of LT electronic faults for both channels)}$$

$$\lambda_{ST-LOTC-AVE} = 65.0 \times 10^{-6} \text{ (failures/hour) (from second electronic faults only)}$$

$$\lambda_{LT-LOTC-AVE} = 50.0 \times 10^{-6} \text{ (failures/hour) (from second electronic faults only)}$$

$$X \text{ (the fraction of undetected faults)} = 0.02$$

$$T_{ST-REPAIR} = 100 \text{ (hours)}$$

$$T_{LT-REPAIR} = \text{To Be Determined to achieve an LOTC rate of } 10 \times 10^{-6} \text{ (events/hour)}$$

$$T_{FL} = 4.5 \text{ (hours)}$$

Substituting the above data into Equation 11, which uses the balanced Equation 6 fractional coefficients, yields the TWA average LOTC rate for an ST repair interval of 100 hours of:

$$\lambda_{LOTC-AVE} = 6.0 \times 10^{-6} + \frac{\{0.20625 + 0.0035 \cdot T_{LT-REPAIR}\} \cdot 10^{-6}}{\{1.003 + 70.0 \times 10^{-6} \cdot T_{LT-REPAIR}\}} \quad (\text{Eq. 11a})$$

A plot showing a comparison of the results from this equation, Equation 11a, with those from the equation used in the original ARP5107 is shown in Figure 5. This plot shows the LOTC rate as a function of the long time repair interval. The short time repair is fixed at 100 hours. As shown, the results using the balanced fractional coefficients from Equation 6 allow a longer LT fault repair interval to be used before the limit (i.e., target) of 10×10^{-6} LOTC rate is encountered. This is because the fractional coefficients contained in this ARP provide a more balanced solution for the times spent in the various dispatch configurations.

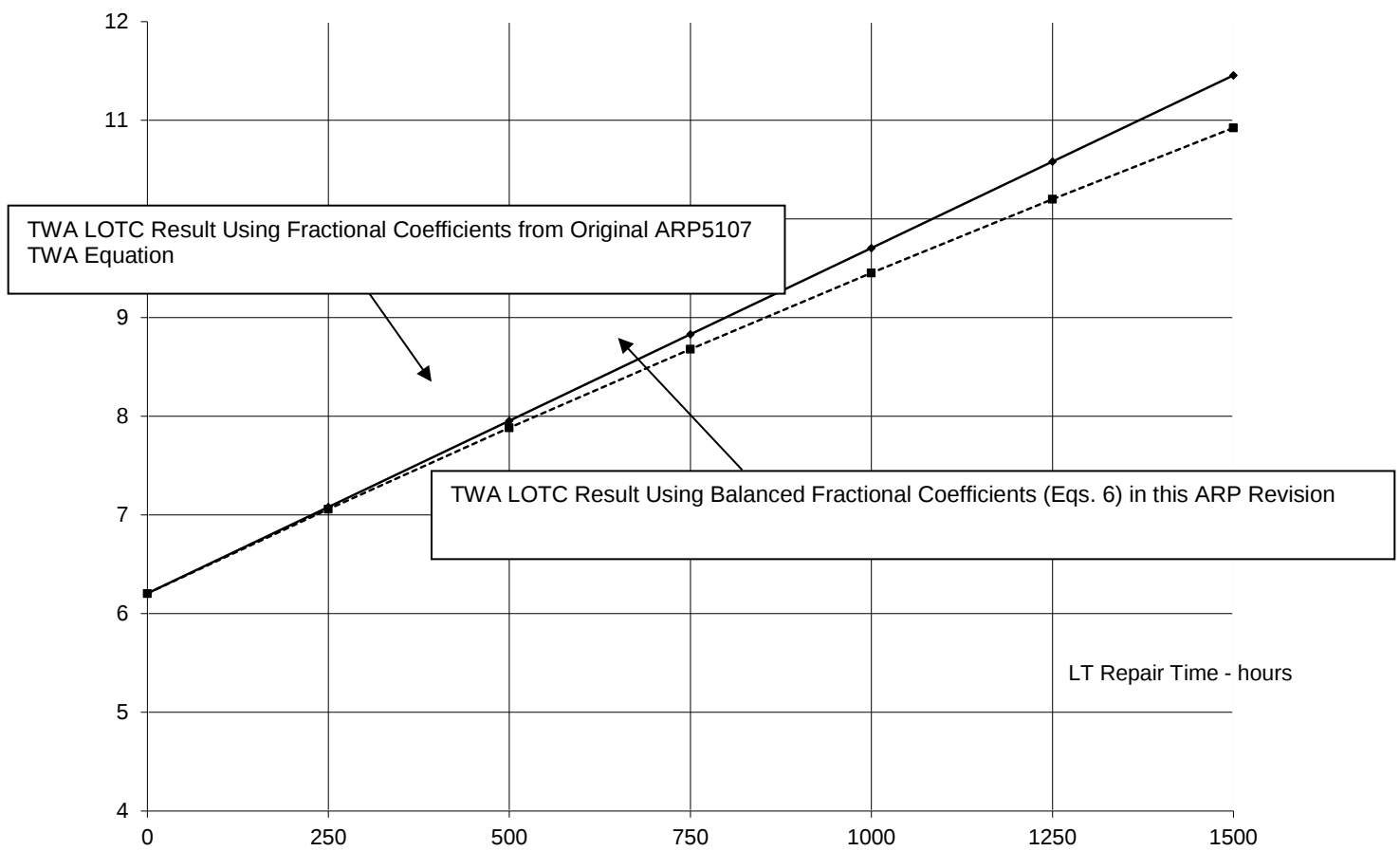


Figure 5 - Plot of the LOTC rate for the example data given in 7.1.5 for both the original fractional coefficients (as given in the original ARP) with the improved fractional coefficients given in this revised ARP

7.2 Markov Model Approach

The Markov modeling (MM) approach is somewhat different than the above TWA approach, but all of the same data is still needed and used.

This document is going to use a unique nomenclature when referring to Markov models, and that nomenclature is to refer to the models as either “open loop” or “closed loop” models. For the purposes of this document, an open loop model is one that has no feedback or simulated repair from the final failed state to the full-up state. And in contrast, closed loop models are those that incorporate a feedback or simulated repair from the fully failed state to the full-up state. Both open and closed loop models can incorporate simulated repair paths from the various faulty states leading to the fully failed state, to the full-up state. Examples of both open loop and closed loop models follow.

7.2.1 Open Loop Markov Models

These models can be visualized as a waterfall system, as shown in Figure 6.

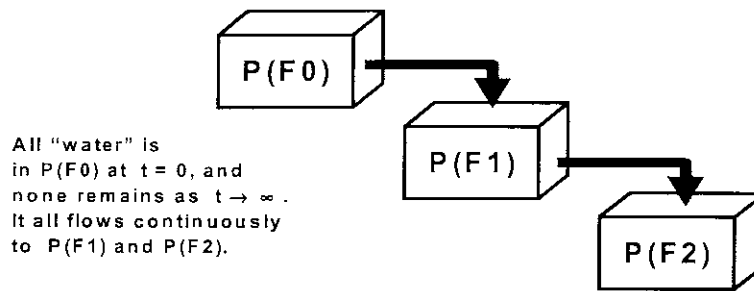


Figure 6 - Open loop Markov model water fall diagram

In this figure, $P(F0)$ represents the probability of being in the full-up state, $P(F1)$ represents the probability of being in the first failure state, and $P(F2)$ is the probability of being in the second failed state, which in this simple model is the final failed state. This is called an "open loop" model herein, because there is no simulated repair path to return any of the water from the fully failed state, $P(F2)$, to the full-up state, $P(F0)$. In open loop models, the initial condition at time zero is usually to have all the water in the full-up state, that is, $P(F0) = 1.0$ at $t = 0.0$. As time increases, the water, or probability, will flow into the first, and then the second failure states. Since there is no simulated repair from the fully failed state, $P(F2)$, to the full-up state, all of the water, or probability, will flow to the final failed state, $P(F2)$, as time approaches infinity. Hence, the probability of being in state $P(F2)$ will approach unity (i.e., 1.0) as time approaches infinity. The model could be revised to incorporate a repair path from the first failed state, $P(F1)$, to the full-up state, but it would still be an open loop model because there is no repair path from the fully failed state to the full-up state. An example of an open loop model with repair paths from initial failure states to the full-up state follows.

A simplified open loop Markov model for a FADEC system is shown in Figure 7.

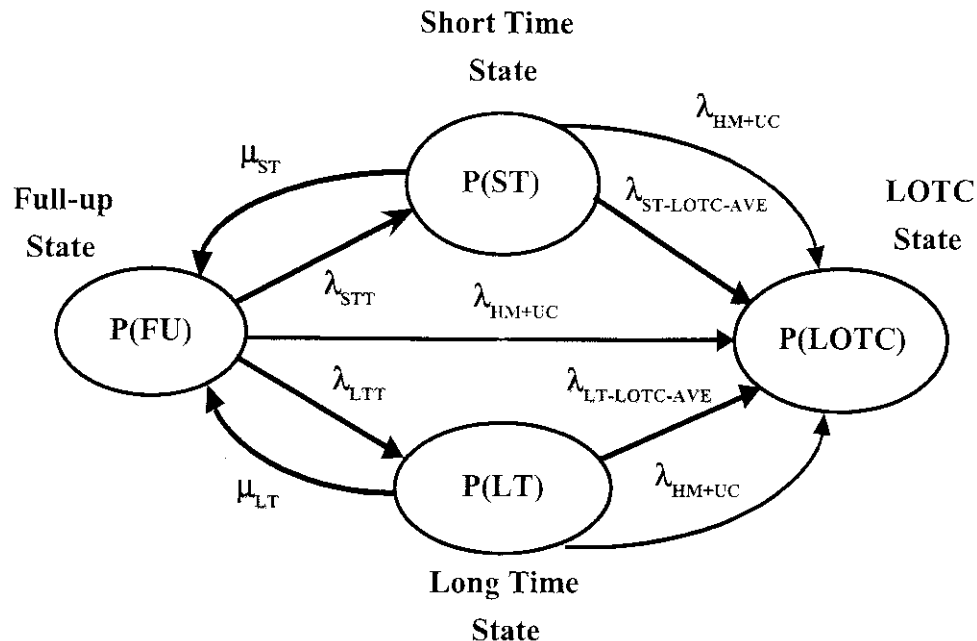


Figure 7 - Open loop Markov model of simple FADEC system with repair for short and long time fault states

It should be noted here that Markov models of FADEC systems normally do not aggregate all short time and long time fault states into one short time and one long time fault state. One could do that, but the various short time and long time fault states (or conditions) are generally shown on a MM diagram (and handled) as separate and independent fault conditions, and they have their own "bubble." If one wishes to aggregate all ST and LT fault states into one ST and one LT state, Equations F7 through F10 in Appendix F show (for single state models) how the λ_{STT} , λ_{LTT} , $\lambda_{ST-LOTC-AVE}$, and $\lambda_{LT-LOTC-AVE}$ rates would be calculated. It is noted that for large repair rates, μ_{ST} and μ_{LT} , with respect to the failure rates into and out of the various ST and LT fault states, the failure rates, λ_{STT} , λ_{LTT} , $\lambda_{ST-LOTC-AVE}$, and $\lambda_{LT-LOTC-AVE}$ approach those values calculated by Equations 3a and 3b, and Equations 8 and 9.

For the purposes of the initial Markov model discussion presented here, the same notation of λ_{STT} , λ_{LTT} , $\lambda_{ST-LOTC-AVE}$, and $\lambda_{LT-LOTC-AVE}$ will be used because it is convenient to show "one" ST state and "one" LT state in these initial model diagrams. As the discussion of Markov models progresses, the actual individual ST and LT states will be shown.

It should also be noted that in a Markov model approach, unlike the TWA approach, the single hydromechanical and undetected fault rate needs to be added to the LOTC rate of each and every fault state, because those single failures can take the system to LOTC from any (and every) fault state.

The μ s represent the repair rates for the states. The repair rate for a repair interval of T hours is usually represented as an exponential transition with a rate of $1/T$ per hour. Hence:

$$\mu_{ST} = 1/T_{ST-REPAIR}, \text{ and}$$

$$\mu_{LT} = 1/T_{LT-REPAIR}$$

In open loop MMs, the solution is obtained by solving a set of first order differential equations which represent the probabilities of being in the various "states." The time-rate-of-change of a probability state is equal to the "probability flow into" that state minus the "probability flow out of" that state. The probability flows into and out of a given state are illustrated in Figure 8.

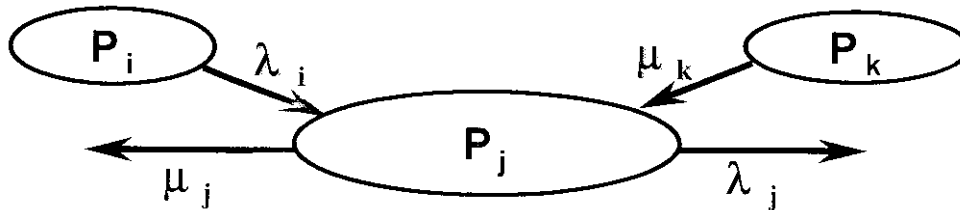


Figure 8 - Probability flow into and out of state P_j

In this figure, the "i" subscript ranges over all of the states that have failures which cause the control to transition into a given P_j state, and the "k" subscript represents all of the states where a repair returns the system to the given P_j state. Referring to this figure, the probability flow into a state is the sum of the failure rates and repair rates into that state multiplied by the respective probabilities of the states driving those failure, and the probability flow out of a state is the sum of the failure rates and repair rates leaving that state multiplied by the probability of the state, itself. Hence, referring to Figure 8:

$$\text{Probability flow into state } P_j \equiv \sum (\lambda_i * P_i) + \sum (\mu_k * P_k)$$

$$\text{Probability flow out of state } P_j \equiv (\mu_j + \lambda_j) * P_j$$

The time dependent differential equation for the P_j state is then, simply:

$$dP_j/dt = \text{Probability flow into state} - \text{Probability flow out of state}$$

$$\text{or, } dP_j/dt = \{ \sum (\lambda_i * P_i) + \sum (\mu_k * P_k) \} - \{ (\mu_j + \lambda_j) * P_j \}$$

Referring to the MM given in Figure 7, the probability flow into the ST state is $\lambda_{STT} * P_{FU}$, which is the transition rate into that state (i.e., λ_{STT}) multiplied by the probability driving that rate, P_{FU} , and the probability flow out of the state is the transition rates, $(\lambda_{ST-LOTC-AVE} + \lambda_{HM+UC} + \mu_{ST})$, multiplied by the probability of the state itself, P_{ST} .

Hence, the time rate of change equation for the ST state shown in Figure 7 is:

$$dP_{ST}/dt = \lambda_{STT} * P_{FU} - (\lambda_{ST-LOTC-AVE} + \mu_{ST} + \lambda_{HM+UC}) * P_{ST}$$

The first order differential equations for the P_{FU} , P_{LT} , and P_{LOTC} states are:

$$dP_{FU}/dt = \mu_{ST} * P_{ST} + \mu_{LT} * P_{LT} - (\lambda_{STT} + \lambda_{LTT} + \lambda_{HM+UC}) * P_{FU}$$

$$dP_{LT}/dt = \lambda_{LTT} * P_{FU} - (\lambda_{LT-LOTC-AVE} + \mu_{LT} + \lambda_{HM+UC}) * P_{LT}$$

$$dP_{LOTC}/dt = \lambda_{HM+UC} * (P_{FU} + P_{ST} + P_{LT}) + \lambda_{ST-LOTC-AVE} * P_{ST} + \lambda_{LT-LOTC-AVE} * P_{LT}$$

These equations define the system.

NOTE: In all Markov models presented herein (and virtually all Markov probability models), one of the probability state equations is redundant and can be derived from the others. To establish an independent set of equations, always eliminate one of the equations - it doesn't matter which one - and add the conservation equation.

The sum of the probabilities of all of probability states must equal unity.

In this example:

$$P_{FU} + P_{ST} + P_{LT} + P_{LOTC} = 1.0$$

Arbitrarily eliminating the first equation, dP_{FU}/dt , and substituting the conservation yields the set of equations representing the MM shown in Figure 7 as:

$$P_{FU} + P_{ST} + P_{LT} + P_{LOTC} = 1.0 \quad (\text{Eq. 12a})$$

$$dP_{ST}/dt = \lambda_{STT} * P_{FU} - (\lambda_{ST-LOTC-AVE} + \mu_{ST} + \lambda_{HM+UC}) * P_{ST} \quad (\text{Eq. 12b})$$

$$dP_{LT}/dt = \lambda_{LTT} * P_{FU} - (\lambda_{LT-LOTC-AVE} + \mu_{LT} + \lambda_{HM+UC}) * P_{LT} \quad (\text{Eq. 12c})$$

$$dP_{LOTC}/dt = \lambda_{HM+UC} * P_{FU} + (\lambda_{ST-LOTC-AVE} + \lambda_{HM+UC}) * P_{ST} + (\lambda_{LT-LOTC-AVE} + \lambda_{HM+UC}) * P_{LT} \quad (\text{Eq. 12d})$$

It is interesting to note that in many papers written on the use of Markov models for solving probability problems, there is no mention of the need to delete one of the equations and substitute the conservation equation to obtain an independent set of equations. Not doing this is acceptable when using the differential equation approach to compute a solution, because the initial conditions for the differential equations would contain the information that the sum of the state probabilities must equal unity, and if the integration algorithm (with time) is accurate, the sum of all state probabilities should remain close to unity. It is still considered that a more robust approach is to eliminate one of the differential equations and replace it with the conservation equation. In the discussion of closed loop Markov models given in 7.2.2, eliminating one of the equations and replacing it with the conservation equation is necessary to achieve a solution.

Using the initial conditions: $P_{FU} = 1.0$, and $P_{ST} = P_{LT} = P_{LOTC} = 0.0$, the set of equations is easily solved to determine the probability states as a function of time.

The overall failure rate of the system, λ_{LOTC} , is then determined from the definition of the hazard rate, which is:

$$\lambda_{LOTC} = (\text{Probability Flow into the } P_{LOTC} \text{ State}) / (1 - P_{LOTC}) \quad (\text{Eq. 13})$$

NOTE: Most references define the "hazard rate" only for non-repairable failure states, in which case the value of "probability flow into a state" equals dP/dt , so the hazard rate takes the familiar form $(dP/dt)/(1-P)$. However, in this document we consider repairable failure states, so it is necessary to use the strict definition of "hazard rate" that distinguishes between the probability flow into and out of the failure states.

Using the Probability flow into the LOTC state, the LOTC rate for this example is:

$$\lambda_{\text{LOTC}} = \frac{\lambda_{\text{HM+UC}} * P_{\text{FU}} + (\lambda_{\text{ST-LOTc-AVE}} + \lambda_{\text{HM+UC}}) * P_{\text{ST}} + (\lambda_{\text{LT-LOTc-AVE}} + \lambda_{\text{HM+UC}}) * P_{\text{LT}}}{(1 - P_{\text{LOTc}})} \quad (\text{Eq. 13a})$$

When solving Equations 12 and calculating the instantaneous LOTC rate from Equation 13a at each point in time, the probabilities of the various states will continuously change with time, but as time approaches infinity (∞) the value of λ_{LOTc} , will approach a constant value. It can be shown that this value asymptotically approaches the smallest eigenvalue of the system, which happens to approximate the long term failure rate under certain conditions. However, in general, it can differ from the true average failure rate of the system by a significant factor, particularly if the repair rates, μ_{ST} and μ_{LT} , are not significantly greater than the failure rates into and out of the ST and LT fault states, respectively. This is discussed and illustrated for a simple 2-unit model in greater detail in Appendix H.

Because of these difficulties, an open loop Markov model is not the preferred modeling approach for determining the average failure rate of a system.

The above difficulties as well as the difficulty of having to solve a set of differential equations is circumvented by using the closed loop Markov model approach.

7.2.2 Closed Loop Markov Model Approach

The closed loop MM approach differs from the open loop approach, only in that a feedback is added from the fully failed state to the full-up state. In this example, from P_{LOTc} to P_{FU} .

The closed loop Markov model diagram for the system is shown in Figure 9.

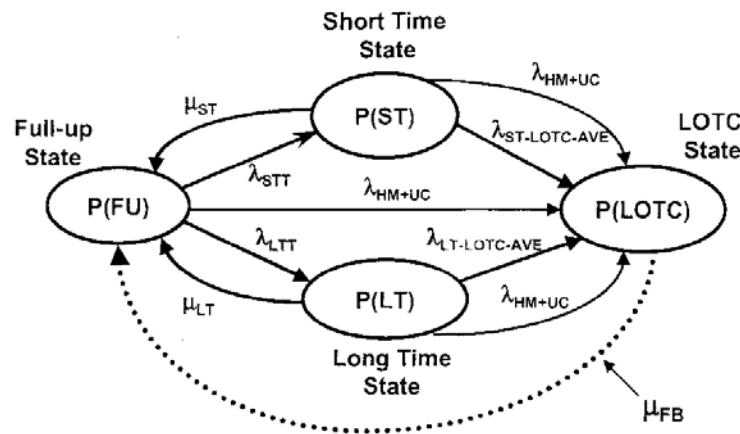


Figure 9 - Closed loop MM for simple FADEC control system with repair for short and long term fault states

The dotted line in Figure 9 represents the feedback path, μ_{FB} , which has been added from the fully failed, P_{LOTc} , state, to the full-up, P_{FU} , state.

Substituting the conservation equation for the dP_{FU}/dt state equation, the system of differential equations for the system is:

$$P_{\text{FU}} + P_{\text{ST}} + P_{\text{LT}} + P_{\text{LOTc}} = 1.0$$

$$dP_{\text{ST}}/dt = \lambda_{\text{STT}} * P_{\text{FU}} - (\lambda_{\text{ST-LOTc-AVE}} + \mu_{\text{ST}} + \lambda_{\text{HM+UC}}) * P_{\text{ST}}$$

$$dP_{\text{LT}}/dt = \lambda_{\text{LTT}} * P_{\text{FU}} - (\lambda_{\text{LT-LOTc-AVE}} + \mu_{\text{LT}} + \lambda_{\text{HM+UC}}) * P_{\text{LT}}$$

$$dP_{\text{LOTc}}/dt = \lambda_{\text{HM+UC}} * (P_{\text{FU}} + P_{\text{ST}} + P_{\text{LT}}) + \lambda_{\text{ST-LOTc-AVE}} * P_{\text{ST}} + \lambda_{\text{LT-LOTc-AVE}} * P_{\text{LT}} - \mu_{\text{FB}} * P_{\text{LOTc}}$$

The only difference between these closed loop equations and those for the open loop MM diagram (Figure 7) is the addition of the $\mu_{FB} * P_{LOTC}$ term to the dP_{LOTC}/dt equation. This term has a negative sign in front of it because it represents the probability flow out of the P_{LOTC} state.

In closed loop models the solution of interest is the steady state solution, because it is the solution which has all of probability states contributing to the fully failed, P_{LOTC} state in a balanced manner, as would be the case in a large fleet of engines.

The steady state solution is obtained by setting all of the dP/dt terms to zero and solving the resulting set of algebraic equations. This makes the calculation of a solution much simpler.

For this example, the set of algebraic equations to be solved is:

$$P_{FU} + P_{ST} + P_{LT} + P_{LOTC} = 1.0 \quad (\text{Eq. 14a})$$

$$0 = \lambda_{STT} * P_{FU} - (\lambda_{ST-LOTC-AVE} + \mu_{ST} + \lambda_{HM+UC}) * P_{ST} \quad (\text{Eq. 14b})$$

$$0 = \lambda_{LTT} * P_{FU} - (\lambda_{LT-LOTC-AVE} + \mu_{LT} + \lambda_{HM+UC}) * P_{LT} \quad (\text{Eq. 14c})$$

$$0 = \lambda_{HM+UC} * P_{FU} + (\lambda_{ST-LOTC-AVE} + \lambda_{HM+UC}) * P_{ST} + (\lambda_{LT-LOTC-AVE} + \lambda_{HM+UC}) * P_{LT} - \mu_{FB} * P_{LOTC} \quad (\text{Eq. 14d})$$

Having estimated the failure rates for the various short time and long time faults, and the failure rates to the LOTC state when operating with those faults, one selects the desired repair rates for short time and long time faults, and solves the above set of algebraic equations to determine the probabilities of being in the various states. A value for μ_{FB} is needed to calculate a solution. Arbitrarily set μ_{FB} to 1.0. The value selected for μ_{FB} will affect the solution, such that different values of μ_{FB} will yield different values for the calculated probabilities of being in the various states, but as is shown below, although the probabilities of being in the various states is a function of μ_{FB} , the failure rate into the LOTC state, λ_{LOTC} , is not a function of μ_{FB} or any of the values of the state probabilities. (An intuitive explanation for why the "feedback" rate doesn't matter is that the overall average failure rate of a fleet of engine control systems is not affected by the length of time a control system is absent from the operational fleet following its failure.)

7.2.2.1 Hazard (or Failure) Rate for a Closed Loop Markov Model

The failure rate equation for the closed loop model of Figure 9 is the same as that (Equation 13a) given for the open loop model of Figure 8. It is repeated here as:

$$\lambda_{LOTC} = \frac{\lambda_{HM+UC} * P_{FU} + (\lambda_{ST-LOTC-AVE} + \lambda_{HM+UC}) * P_{ST} + (\lambda_{LT-LOTC-AVE} + \lambda_{HM+UC}) * P_{LT}}{(1 - P_{LOTC})} \quad (\text{Eq. 15})$$

It would certainly appear that failure rate given by Equation 15 is a function of the state probabilities, but the following will show that it isn't.

7.2.2.2 Reorganizing the Failure Rate Equation

Rearranging Equation 14a yields:

$$1 - P_{LOTC} = P_{FU} + P_{ST} + P_{LT}$$

Substituting this into the denominator of Equation 15 yields:

$$\lambda_{LOTC} = \frac{\lambda_{HM+UC} * P_{FU} + (\lambda_{ST-LOTC-AVE} + \lambda_{HM+UC}) * P_{ST} + (\lambda_{LT-LOTC-AVE} + \lambda_{HM+UC}) * P_{LT}}{P_{FU} + P_{ST} + P_{LT}} \quad (\text{Eq. 16})$$

And Equations 14b and 14c can be rearranged to solve for P_{ST} and P_{LT} as a function of P_{FU} :

$$PST = \lambda_{STT} * PFU / (\mu_{ST} + \lambda_{ST-LOT C-AVE} + \lambda_{HM+UC})$$

$$PLT = \lambda_{LTT} * PFU / (\mu_{LT} + \lambda_{LT-LOT C-AVE} + \lambda_{HM+UC})$$

Substituting Equations 17a and 17b into Equation 16 for PST and PLT yields:

$$\lambda_{LOT C} = \frac{\lambda_{STT} * (\lambda_{ST-LOT C-AVE} + \lambda_{HM+UC})}{\mu_{ST} + \lambda_{ST-LOT C-AVE} + \lambda_{HM+UC}} + \frac{\lambda_{LTT} * (\lambda_{LT-LOT C-AVE} + \lambda_{HM+UC})}{\mu_{LT} + \lambda_{LT-LOT C-AVE} + \lambda_{HM+UC}} \quad (Eq. 18)$$

$$1.0 + \frac{\lambda_{STT}}{\mu_{ST} + \lambda_{ST-LOT C-AVE} + \lambda_{HM+UC}} + \frac{\lambda_{LTT}}{\mu_{LT} + \lambda_{LT-LOT C-AVE} + \lambda_{HM+UC}}$$

NOTE: This equation only involves the failure rates and repair rates of the system, and that it is independent of the feedback rate μ_{FB} and all state probabilities. This is a highly desirable characteristic of closed loop, single state MMs.

7.2.2.3 Single State Closed Loop MMs

For the purposes of this ARP a single state MM is one which shows only single fault conditions as individual states. All second faults from the single states lead to the LOTC state. Second faults, which do not lead to the LOTC state, are not modeled. Hence, no dual state fault conditions are shown as separate states. Therefore, the transition rates from the single failure states represent only those additional single failures that would take the system from the single faulty states to the LOTC state. A generic single state MM for a FADEC system is shown in Figure 10.

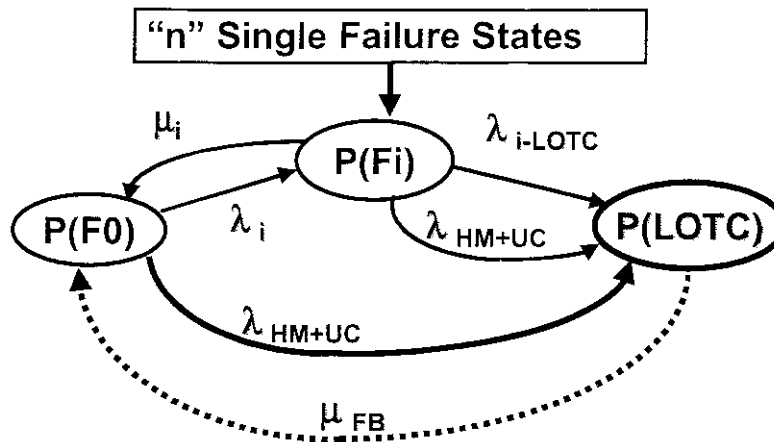


Figure 10 - Single state Markov model

The n single fault states can be ST or LT states, or No Dispatch states, when the No Dispatch (ND) condition does not result in an LOTC event. The repair rates, μ_i , for the ST and LT states are the reciprocals of the ST and LT repair times. For the ND states, the repair time is normally set to the reciprocal of $\frac{1}{2}$ of the average flight time. This is because it is assumed that the system would enter an ND state approximately half-way through the flight. There are control systems that have single failures which result in an ND state, but do not necessarily lead to an LOTC event. Examples of these control systems are ones with only one P_B (i.e., burner pressure) or P_{amb} (i.e., ambient pressure) sensor. Loss of these sensors may not cause an LOTC event, but may result in an ND condition. However, in most systems ND states are usually not modeled in a single state Markov model because it would normally take two independent fault conditions to get into a non-dispatchable state (or configuration), and hence, a single state model would not, by definition, model these conditions.

7.2.2.4 Two Generalized Solution Equations for Single State Models

The general form of the solution for this model is given by Equation 19.

$$\lambda_{\text{LOT C}} = \frac{\lambda_{\text{HM+UC}} + \sum \{ (\lambda_i * (\lambda_{\text{i-LOT C}} + \lambda_{\text{HM+UC}}) / (\mu_i + \lambda_{\text{i-LOT C}} + \lambda_{\text{HM+UC}})) \}}{1.0 + \sum \{ \lambda_i / (\mu_i + \lambda_{\text{i-LOT C}} + \lambda_{\text{HM+UC}}) \}} \quad (\text{Eq. 19})$$

where:

$\lambda_{\text{HM+UC}}$ represents the hydromechanical plus undetected fault rate.

λ_i represents the failure rate from the full-up state to a given fault state.

$\lambda_{\text{i-LOT C}}$ is that failure rate from that given single fault state to the LOTC state, due to additional single faults in the redundant portions of the electronic control. (This failure rate does not include the single element hydromechanical and undetected faults, as these faults are accounted in the $\lambda_{\text{HM+UC}}$ term.)

μ_i is the repair rate for the fault state.

A slightly different nomenclature is often used. In this representation, the failure rate from the single failure states to the LOTC state, $\lambda_{\text{i-LOT C}}$, includes the additional $\lambda_{\text{HM+UC}}$ failure rate term. That is:

$$\lambda_{\text{i-LOT C+HM+UC}} = \lambda_{\text{i-LOT C}} + \lambda_{\text{HM+UC}}$$

When this is done, Equation 19 takes the form:

$$\lambda_{\text{LOT C}} = \frac{\lambda_{\text{HM+UC}} + \sum \{ (\lambda_i * \lambda_{\text{i-LOT C+HM+UC}}) / (\mu_i + \lambda_{\text{i-LOT C+HM+UC}}) \}}{1.0 + \sum \{ \lambda_i / (\mu_i + \lambda_{\text{i-LOT C+HM+UC}}) \}} \quad (\text{Eq. 20})$$

Equation 19 and Equation 20 are exactly the same. They just use different nomenclature for the failure rates from the single failure states to the LOTC state.

7.2.2.5 First Order Approximation to the Single Fault Markov Model LOTC Equation (Equations 20)

A difficulty with Equations 19 and 20 is that when computing the LOTC rate using a spread sheet approach, which is done in the example FADEC system discussed in 7.4 and shown in Table 1, one has to continually re-do the summations shown in the numerator and denominator of those equations for each new value of μ_{LT} to obtain the data for plotting the LOTC rate as a function of the long time repair interval. This difficulty can be eliminated by approximating the summations $\sum \{ (\lambda_i * \lambda_{\text{i-LOT C+HM+UC}}) / (\mu_i + \lambda_{\text{i-LOT C+HM+UC}}) \}$ and $\sum \{ \lambda_i / (\mu_i + \lambda_{\text{i-LOT C+HM+UC}}) \}$ with simple, first order expansions.

First, replace the repair rate, μ_i , with the repair interval, T_i . Equation 20 then becomes:

$$\lambda_{\text{LOT C}} = \frac{\lambda_{\text{HM+UC}} + \sum \{ (\lambda_i * \lambda_{\text{i-LOT C+HM+UC}} * T_i) / (1 + \lambda_{\text{i-LOT C+HM+UC}} * T_i) \}}{1.0 + \sum \{ \lambda_i / (1 + \lambda_{\text{i-LOT C+HM+UC}} * T_i) \}} \quad (\text{Eq. 20a})$$

The first order approximations for the summations are:

$$\sum \{ (\lambda_i * \lambda_{\text{i-LOT C+HM+UC}} * T_i) / (1 + \lambda_{\text{i-LOT C+HM+UC}} * T_i) \} \approx \sum (\lambda_i * \lambda_{\text{i-LOT C+HM+UC}} * T_i) - \sum (\lambda_i * (\lambda_{\text{i-LOT C+HM+UC}} * T_i)^2)$$

$$\sum \{ \lambda_i / (1 + \lambda_{\text{i-LOT C+HM+UC}} * T_i) \} \approx \sum (\lambda_i * T_i) - \sum (\lambda_i * \lambda_{\text{i-LOT C+HM+UC}} * T_i^2)$$

Substituting these approximations into Equation 20a yields the approximation:

$$\lambda_{\text{LOTc}} \approx \frac{\lambda_{\text{HM+UC}} + \sum(\lambda_i * \lambda_{i-\text{LOTc}+\text{HM+UC}} * T_i) - \sum(\lambda_i * (\lambda_{i-\text{LOTc}+\text{HM+UC}} * T_i)^2)}{1.0 + \sum(\lambda_i * T_i) - \sum(\lambda_i * \lambda_{i-\text{LOTc}+\text{HM+UC}} * T_i^2)} \quad (\text{Eq. 20b})$$

Equation 20b may not look any simpler than Equation 20a, but when T_i is a fixed value for a group of faults, the summations for the “ λ ” terms for that group of faults only has to be done once. For example, if all single fault states are to be grouped into a short time or long time repair group with repair intervals of T_{ST} and T_{LT} , respectively, approximation 20b becomes:

$$\lambda_{\text{LOTc}} \approx \frac{\lambda_{\text{HM+UC}} + a_0 * T_{\text{ST}} - a_1 * T_{\text{ST}}^2 + c_0 * T_{\text{LT}} - c_1 * T_{\text{LT}}^2}{1.0 + b_0 * T_{\text{ST}} - b_1 * T_{\text{ST}}^2 + d_0 * T_{\text{LT}} - d_1 * T_{\text{LT}}^2} \quad (\text{Eq. 20c})$$

where:

$$a_0 = \sum(\lambda_{\text{STi}} * \lambda_{\text{STi-LOTc}+\text{HM+UC}})$$

$$a_1 = \sum(\lambda_{\text{STi}} * (\lambda_{\text{STi-LOTc}+\text{HM+UC}})^2)$$

$$b_0 = \sum(\lambda_{\text{STi}})$$

$$b_1 = a_0$$

$$c_0 = \sum(\lambda_{\text{LTi}} * \lambda_{\text{LTi-LOTc}+\text{HM+UC}})$$

$$c_1 = \sum(\lambda_{\text{LTi}} * (\lambda_{\text{LTi-LOTc}+\text{HM+UC}})^2)$$

$$d_0 = \sum(\lambda_{\text{LTi}})$$

$$d_1 = c_0$$

These coefficients only have to be calculated once for the fault states in the ST and LT fault groups, and then the repair intervals, T_{ST} and T_{LT} can be varied to determine the effect on the LOTC rate.

7.2.2.6 Simplified Approximations When Using High Repair Rates (i.e., Short Repair Intervals)

In Equations 19 and 20, the $(\lambda_{i-\text{LOTc}} + \lambda_{\text{HM+UC}})$ and $\lambda_{i-\text{LOTc}+\text{HM+UC}}$ terms, which represent the same failure rates, are usually less than $50 * 10^{-06}$, and the repair rates, μ_i , are generally greater than 0.001 (i.e., repair times of less than 1000 hours in a time-since-fault-model). Therefore, the μ_i 's are approximately 10 times greater than the $\lambda_{i-\text{LOTc}+\text{HM+UC}}$ failure rates. This being the case, Equations 19 and 20 can be simplified to:

$$\lambda_{\text{LOTc}} = \frac{\lambda_{\text{HM+UC}} + \sum\{(\lambda_i * (\lambda_{i-\text{LOTc}} + \lambda_{\text{HM+UC}}) / \mu_i)\}}{1.0 + \sum\{\lambda_i / \mu_i\}} \quad (\text{Eq. 19a})$$

and

$$\lambda_{\text{LOTc}} \approx \frac{\lambda_{\text{HM+UC}} + \sum(\lambda_i * \lambda_{i-\text{LOTc}+\text{HM+UC}} / \mu_i)}{1.0 + \sum(\lambda_i / \mu_i)} \quad (\text{Eq. 20d})$$

Again, these two equations yield the same answer. The only difference in the equations is whether the HMU plus undetected fault rate is included in the failure rates from the single faulty states to the LOTC state, as it is in Equations 20, 20a, 20b, etc., or whether the HMU plus undetected failure rate is not included in the $\lambda_{i-\text{LOTc}}$ failure rate but handled separately, as is done in Equations 19 and 19a.

Since $(1/\mu_i)$ is simply the repair time for a particular fault repair interval, $T_{i-REPAIR}$, Equation 20d can be written as:

$$\lambda_{LOT C} \approx \frac{\lambda_{HM+UC} + \sum (T_{i-REPAIR} * \lambda_i * \lambda_{i-LOT C+HM+UC})}{1.0 + \sum (T_{i-REPAIR} * \lambda_i)} \quad (\text{Eq. 20e})$$

When the dispatchable faults are allocated to two fault groups, a short time fault group with a repair time of T_{ST} and a long time fault group with repair time T_{LT} , Equation 20a can be written as:

$$\lambda_{LOT C} \approx \frac{\lambda_{HM+UC} + T_{ST} * \sum (\lambda_{STi} * \lambda_{STi-LOT C+HM+UC}) + T_{LT} * \sum (\lambda_{LTi} * \lambda_{LTi-LOT C+HM+UC})}{1.0 + T_{ST} * \sum (\lambda_{STi}) + T_{LT} * \sum (\lambda_{LTi})} \quad (\text{Eq. 20f})$$

Generally, when the time-since-fault repair times are less than 1000 hours, Equation 20e (and Equation 20f when there are just two fault groups) yield reasonably good approximations for the estimated LOTC failure rate. If repair times of 1000 hours or more are to be considered, the analyst can revert to the use of Equation 20, 20a, or 20b. (Note: The 1000-hour long time repair time is not to be considered an absolute number. It's a relative number. As discussed in 7.2.4, the repair rate, which is the reciprocal of the repair interval, has to be at least 10 times greater than the failure rates into and out of the various fault states for single state models to be reasonably accurate.)

7.2.3 Examples of Single Fault States

Examples of single failure states in an engine FADEC system are operation with one item, such as a T2, $P_{ambient}$ or other sensor failed; a fuel metering valve or variable geometry feedback failed; a CPU or power supply in one channel failed; or any other single failure being modeled.

7.2.4 Acceptability (and Accuracy) of Single State Models

In general, single fault state models are acceptable when the repair rate for the single fault states are approximately 10 times (or more) greater than the maximum failure rate into or out of those fault states. Most Markov models group the dispatchable faults conditions into either a short time (ST) or long time (LT) repair category. For these models to be reasonably accurate (i.e., approximately 5%), the repair rate for all ST fault states should be at least 10 times greater than the maximum failure rate into or out of any given ST fault state, and, similarly, the repair rate for all LT fault states should be at least 10 times greater than the maximum failure rate into or out of any given LT fault state. Making the repair rates for the first fault states high translates into making multiple faults so improbable that they are negligible contributors to the shutdown rate. This is why high repair rates ensures that a "single state" model is reasonably accurate. See Appendix G for further discussion of this subject.

7.3 Comparison of TWA and MM Approaches

A comparison of the TWA and MM solutions for the example system given in 7.1.5 is shown in Figure 11.

The two TWA solutions shown in Figure 11 are the same as those shown in Figure 5. The MM results using Equations 20, 20c, and 20f are also shown. Note that the TWA solution using the balanced fractional coefficients from this ARP (Equation 6) is virtually the same as the simplified (Equation 20f) Markov Model solution - and both the balanced fractional coefficient solution and the simplified MM solution from Equation 20e (i.e., Equation 20f for a system for two fault groups) are easier to calculate than the MM solution given by Equation 20, as the coefficients only have to be calculated once.

If one desires a very good match to the full Markov model solution given by Equation 20 - but without the need to re-do the spread sheet when the repair times are changed - the first order approximation given by Equation 20c should be used. The coefficients a_0 , a_1 , b_0 , b_1 , c_0 , c_1 , d_0 , and d_1 used in the approximation, Equation 20c, only have to be calculated once, and there are only two more of these coefficients than in the simplified Equation 20f solution.

All of the solution methods provide acceptable accuracy. The preferred approach is to use the first order approximation given by Equation 20c. It provides an excellent approximation to the full Markov model solution equation with significantly less effort.

7.4 A Single State FADEC System MM Example

A single state MM for an example FADEC system is shown in Figure 12. In this system, the bleed valves account for much of the single element mechanical failure rate, and since they are all controlled separately by the electronics, they contribute a significant portion to the electrical/electronic system's failure rate. The EEC and alternator were put into the ST repair state because when either is failed, it takes away a significant amount of redundancy. All other items were placed into the LT category.

In this particular system, the N1 and N2 sensor systems are triple and quad redundant, respectively, and the control is not dispatchable without two of each of these signals present, so the impact on the LOTC rate from a complete loss of N1 or N2 is negligible.

7.4.1 Description of the Excel Spreadsheet Data

The following is an example of using a spread sheet to obtain the estimated LOTC rate for the FADEC system represented by the single state Markov model shown in Figure 12. The spread sheet solution uses Equation 20 to approximate the LOTC rate.

In referring to the Excel spread sheets shown in Table 1 below:

Column A is simply the row number. This has nothing to do with any of the calculations.

Column B lists the fault states.

Column C is λ_i , the failure rate from the full-up state into that fault state.

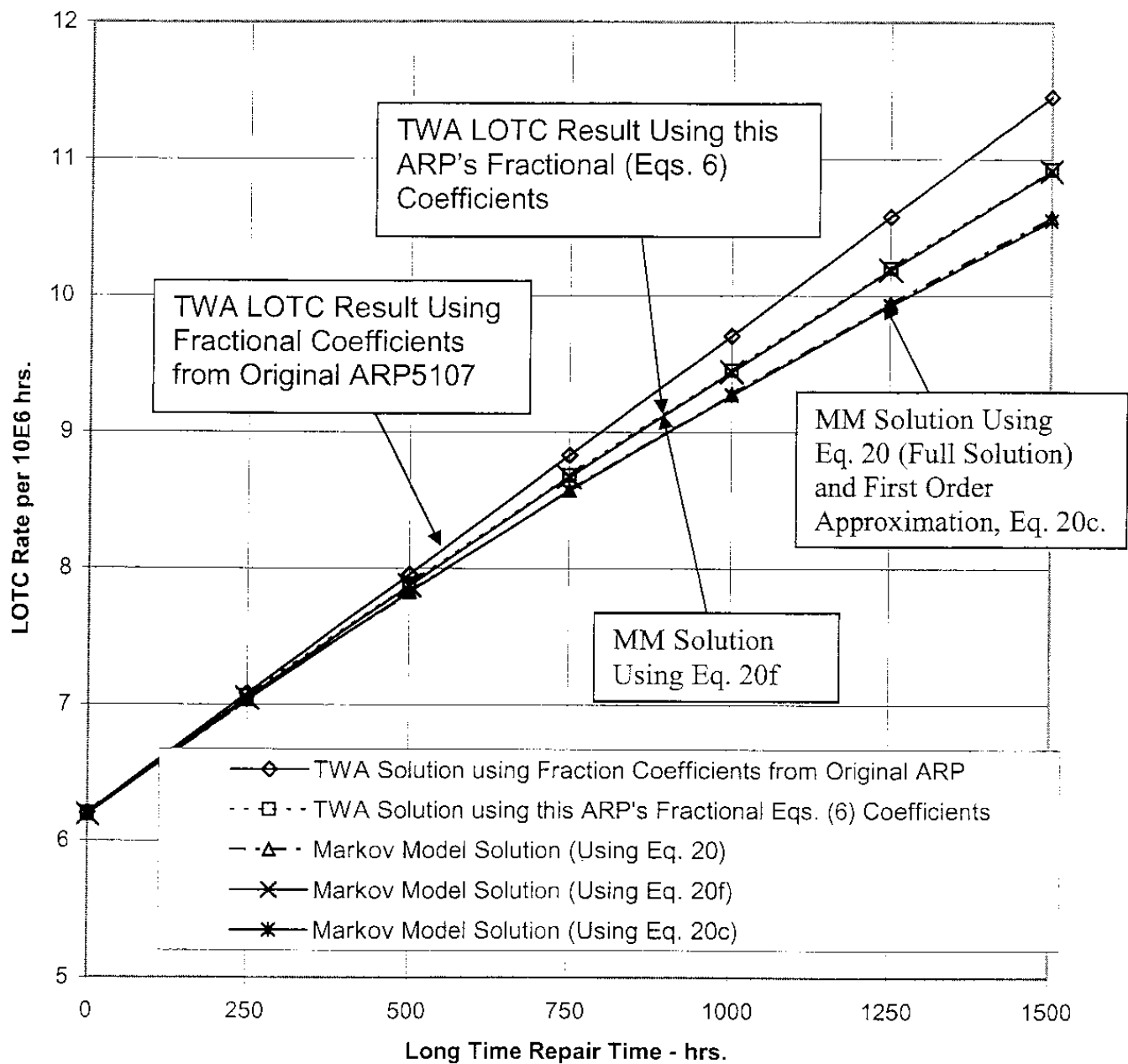


Figure 11 - Comparison of TWA solutions using the original ARP fractional coefficients and the balanced Equation 6 coefficients of this ARP with Markov model solutions using Equations 20, 20c, and 20f (from this ARP) for the FADEC system data given in 7.1.5

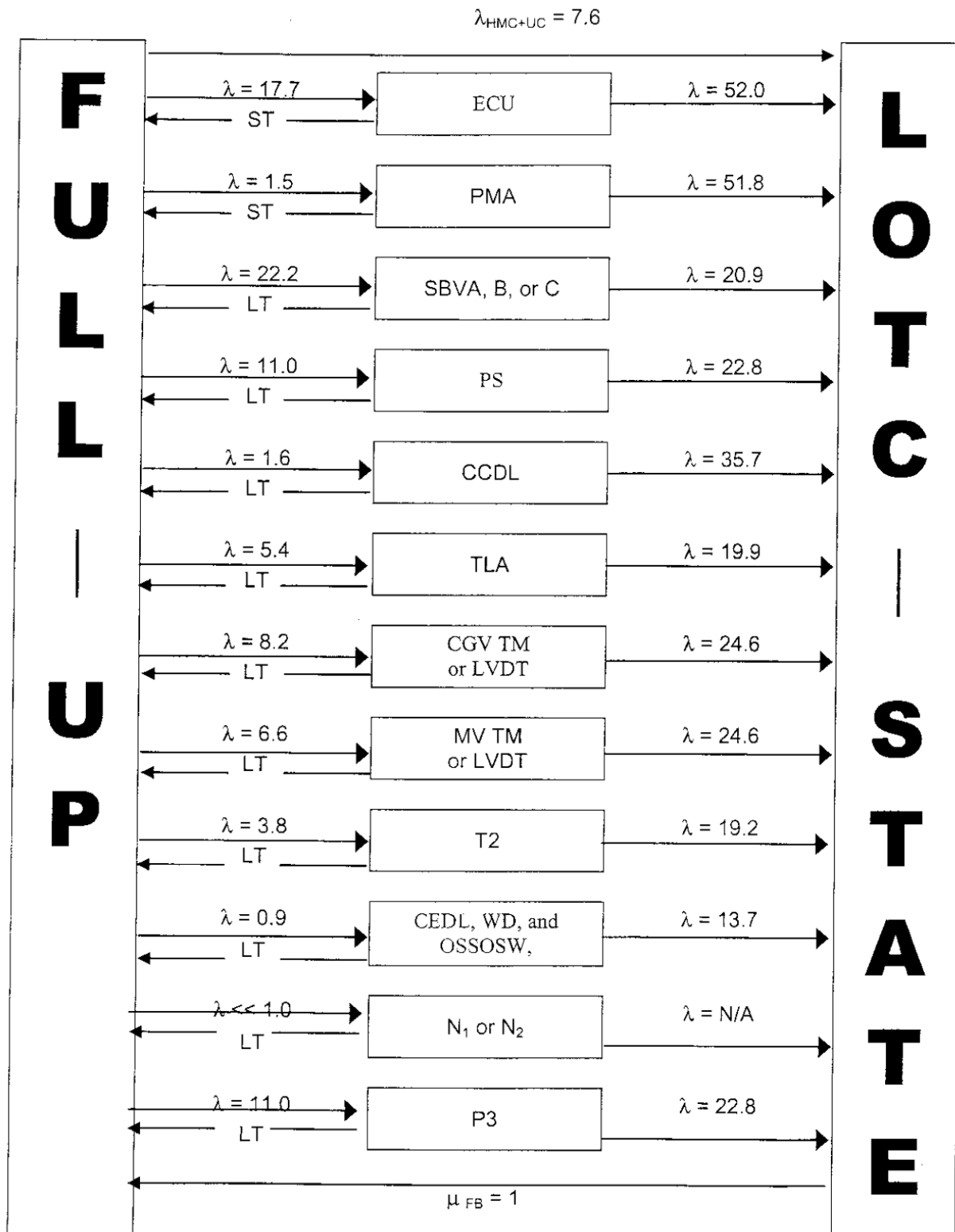


Figure 12 - MM diagram of a typical FADEC system
 (Note: All λ 's are failures per million hours)

Column D is $\lambda_{i-LOTCH+HM+UC}$, the failure rate from that state into the LOTC state. This rate includes the single element HMU and undetected failure rate, as well as the additional (single) electrical/electronic failures in the redundant elements of the control that would take the system to the LOTC state (i.e., result in an LOTC event).

Column E is $\lambda_i/(\mu_i + \lambda_{i-LOTCH+HM+UC})$, where μ_i is the appropriate repair rate (i.e., $1/T_{REPAIR}$) for that state.

Column F is $(\lambda_{i-LOTCH+HM+UC} * \lambda_i)/(\mu_i + \lambda_{i-LOTCH+HM+UC})$, which is simply column D times column E.

The rate for the single mechanical/hydraulic element failures and electrical/electronic failures that cause the system go directly from the full-up state (and any other fault state) to the LOTC state is 7.6 per million hours.

The short time repair interval used in the analysis is fixed at 250 hours. This is because the applicant wishes to obtain an ST dispatch interval of 125 hours, and since the system being analyzed is for an "initial FADEC system application," the analysis is completed using a margin of 2, which is required by the current FAA TLD Policy Letter.

$$\text{Column G, LOTC rate is } = \frac{[0.0000076 + \sum((\lambda_{i-LOTCH+HM+UC} * \lambda_i)/(\mu_i + \lambda_{i-LOTCH+HM+UC}))]}{1 + \sum(\lambda_i / (\mu_i + \lambda_{i-LOTCH+HM+UC}))}$$

$$\text{for example, } G22 = [0.0000076 + F8 + F22] / [1. + E8 + E22]$$

$$\text{and } G37 = [0.0000076 + F8 + F37] / [1. + E8 + E37]$$

$$\text{and } G52 = [0.0000076 + F8 + F52] / [1. + E8 + E52]$$

$$\text{and } G67 = [0.0000076 + F8 + F67] / [1. + E8 + E67]$$

$$\text{and } G82 = [0.0000076 + F8 + F82] / [1. + E8 + E82]$$

The F8 and E8 terms always stay the same because those terms are for the short time repair faults and the time for those fault states is fixed at 250 hours.

Table 2 - Spreadsheet solution for FADEC system example shown in Figure 12

$$T_{ST-Repair} = 250 \text{ hours } (\mu_{ST} = 0.004 \text{ events/hour})$$

A	B	C	D	E	F	G
		λ_i	$\lambda_{i-LOTCH+HM+UC}$	$\lambda_i / (\mu_{ST} + \lambda_{i-LOTCH+HM+UC})$	$(\lambda_{i-LOTCH+HM+UC} * \lambda_i) / (\mu_{ST} + \lambda_{i-LOTCH+HM+UC})$	
4	CPU (system)	1.77E-05	5.20E-05	4.37E-03	2.27E-07	
5	PMA	1.50E-06	5.18E-05	3.70E-04	1.92E-08	
6						
7				SUM	SUM	
8				4.74E-03	2.46E-07	

$T_{LT-Repair} = 1 \text{ hour}$ ($\mu_{LT} = 1.0 \text{ events/hour}$)

A	B	C	D	E	F	G
		λ_i	$\lambda_{i-LOTCH+HM+UC}$	$\lambda_i / (\mu_{LT} + \lambda_{i-LOTCH+HM+UC})$	$(\lambda_{i-LOTCH} * \lambda_i) / (\mu_{LT} + \lambda_{i-LOTCH+HM+UC})$	λ_{LOTCH}
11	SBV A,B,C	2.22E-05	2.09E-05	2.22E-05	4.64E-10	
12	PS	1.10E-05	2.28E-05	1.10E-05	2.51E-10	
13	CCDL	1.60E-06	3.57E-05	1.60E-06	5.71E-11	
14	TLA	5.40E-06	1.99E-05	5.40E-06	1.07E-10	
15	CGV	8.20E-06	2.46E-05	8.20E-06	2.02E-10	
16	MV	6.60E-06	2.46E-05	6.60E-06	1.62E-10	
17	T2	3.80E-06	1.92E-05	3.80E-06	7.30E-11	
18	4 SUMS	9.00E-07	1.37E-05	9.00E-07	1.23E-11	
19	P3	1.10E-05	2.28E-05	1.10E-05	2.51E-10	
20						
21				SUM	SUM	
22				7.07E-05	1.58E-09	7.81E-06

$T_{LT-Repair} = 1000 \text{ hours}$ ($\mu_{LT} = 0.001 \text{ events/hour}$)

A	B	C	D	E	F	G
		λ_i	$\lambda_{i-LOTCH+HM+UC}$	$\lambda_i / (\mu_{LT} + \lambda_{i-LOTCH+HM+UC})$	$(\lambda_{i-LOTCH+HM+UC} * \lambda_i) / (\mu_{LT} + \lambda_{i-LOTCH+HM+UC})$	λ_{LOTCH}
26	SBV A,B,C	2.22E-05	2.09E-05	2.17E-02	4.54E-07	
27	PS	1.10E-05	2.28E-05	1.08E-02	2.45E-07	
28	CCDL	1.60E-06	3.57E-05	1.54E-03	5.52E-08	
29	TLA	5.40E-06	1.99E-05	5.29E-03	1.05E-07	
30	CGV	8.20E-06	2.46E-05	8.00E-03	1.97E-07	
31	MV	6.60E-06	2.46E-05	6.44E-03	1.58E-07	
32	T2	3.80E-06	1.92E-05	3.73E-03	7.16E-08	
33	4 SUMS	9.00E-07	1.37E-05	8.88E-04	1.22E-08	
34	P3	1.10E-05	2.28E-05	1.08E-02	2.45E-07	
35						
36				SUM	SUM	
37				6.92E-02	1.54E-06	8.74E-06

$T_{LT-Repair} = 2000$ hours ($\mu_{LT} = 0.0005$ events/hour)

A	B	C	D	E	F	G
		λ_i	$\lambda_{i-LOTCH+HM+UC}$	$\lambda_i / (\mu_{LT} + \lambda_{i-LOTCH+HM+UC})$	$(\lambda_{i-LOTCH+HM+UC} * \lambda_i) / (\mu_{LT} + \lambda_{i-LOTCH+HM+UC})$	λ_{LOTCH}
41	SBV A,B,C	2.22E-05	2.09E-05	4.26E-02	8.91E-07	
42	PS	1.10E-05	2.28E-05	2.10E-02	4.80E-07	
43	CCDL	1.60E-06	3.57E-05	2.99E-03	1.07E-07	
44	TLA	5.40E-06	1.99E-05	1.04E-02	2.07E-07	
45	CGV	8.20E-06	2.46E-05	1.56E-02	3.85E-07	
46	MV	6.60E-06	2.46E-05	1.26E-02	3.09E-07	
47	T2	3.80E-06	1.92E-05	7.32E-03	1.41E-07	
48	4 SUMS	9.00E-07	1.37E-05	1.75E-03	2.40E-08	
49	P3	1.10E-05	2.28E-05	2.10E-02	4.80E-07	
50						
51				SUM	SUM	
52				1.35E-01	3.02E-06	9.53E-06

$T_{LT-Repair} = 3000$ hours ($\mu_{LT} = 0.000333$ events/hour)

A	B	C	D	E	F	G
		λ_i	$\lambda_{i-LOTCH+HM+UC}$	$\lambda_i / (\mu_{LT} + \lambda_{i-LOTCH+HM+UC})$	$(\lambda_{i-LOTCH+HM+UC} * \lambda_i) / (\mu_{LT} + \lambda_{i-LOTCH+HM+UC})$	λ_{LOTCH}
56	SBV A,B,C	2.22E-05	2.09E-05	6.27E-02	1.31E-06	
57	PS	1.10E-05	2.28E-05	3.09E-02	7.04E-07	
58	CCDL	1.60E-06	3.57E-05	4.34E-03	1.55E-07	
59	TLA	5.40E-06	1.99E-05	1.53E-02	3.04E-07	
60	CGV	8.20E-06	2.46E-05	2.29E-02	5.64E-07	
61	MV	6.60E-06	2.46E-05	1.84E-02	4.54E-07	
62	T2	3.80E-06	1.92E-05	1.08E-02	2.07E-07	
63	4 SUMS	9.00E-07	1.37E-05	2.59E-03	3.55E-08	
64	P3	1.10E-05	2.28E-05	3.09E-02	7.04E-07	
65						
66				SUM	SUM	
67				1.99E-01	4.44E-06	1.021E-05

$T_{LT-Repair} = 4000$ hours ($\mu_{LT} = 0.00025$ events/hour)

A	B	C	D	E	F	G
		λ_i	$\lambda_{i-LOTCH+HM+UC}$	$\lambda_i / (\mu_{LT} + \lambda_{i-LOTCH+HM+UC})$	$(\lambda_{i-LOTCH+HM+UC} * \lambda_i) / (\mu_{LT} + \lambda_{i-LOTCH+HM+UC})$	λ_{LOTCH}
71	SBV A,B,C	2.22E-05	2.09E-05	8.19E-02	1.71E-06	
72	PS	1.10E-05	2.28E-05	4.03E-02	9.19E-07	
73	CCDL	1.60E-06	3.57E-05	5.60E-03	2.00E-07	
74	TLA	5.40E-06	1.99E-05	2.00E-02	3.98E-07	
75	CGV	8.20E-06	2.46E-05	2.99E-02	7.35E-07	
76	MV	6.60E-06	2.46E-05	2.40E-02	5.91E-07	
77	T2	3.80E-06	1.92E-05	1.41E-02	2.71E-07	
78	4 SUMS	9.00E-07	1.37E-05	3.41E-03	4.68E-08	
79	P3	1.10E-05	2.28E-05	4.03E-02	9.19E-07	
80						
81				SUM	SUM	
82				2.60E-01	5.79E-06	1.079E-05

$T_{LT-Repair} = 5000$ hours ($\mu_{LT} = 0.0002$ events/hour)

A	B	C	D	E	F	G
		λ_i	$\lambda_{i-LOTCH+HM+UC}$	$\lambda_i / (\mu_{LT} + \lambda_{i-LOTCH+HM+UC})$	$(\lambda_{i-LOTCH+HM+UC} * \lambda_i) / (\mu_{LT} + \lambda_{i-LOTCH+HM+UC})$	λ_{LOTCH}
86	SBV A,B,C	2.22E-05	2.09E-05	1.00E-01	2.10E-06	
87	PS	1.10E-05	2.28E-05	4.94E-02	1.13E-06	
88	CCDL	1.60E-06	3.57E-05	6.79E-03	2.42E-07	
89	TLA	5.40E-06	1.99E-05	2.46E-02	4.89E-07	
90	CGV	8.20E-06	2.46E-05	3.65E-02	8.98E-07	
91	MV	6.60E-06	2.46E-05	2.94E-02	7.23E-07	
92	T2	3.80E-06	1.92E-05	1.73E-02	3.33E-07	
93	4 SUMS	9.00E-07	1.37E-05	4.21E-03	5.77E-08	
94	P3	1.10E-05	2.28E-05	4.94E-02	1.13E-06	
95						
96				SUM	SUM	
97				3.18E-01	7.09E-06	1.130E-05

$T_{LT-Repair} = 6000$ hours ($\mu_{LT} = 0.0001667$ events/hour)

A	B	C	D	E	F	G
		λ_i	$\lambda_{i-LOTCHM+UC}$	$\lambda_i / (\mu_{LT} + \lambda_{i-LOTCHM+UC})$	$(\lambda_{i-LOTCHM+UC} * \lambda_i) / (\mu_{LT} + \lambda_{i-LOTCHM+UC})$	λ_{LOTCH}
101	SBV A,B,C	2.22E-05	2.09E-05	1.18E-01	2.47E-06	
102	PS	1.10E-05	2.28E-05	5.81E-02	1.32E-06	
103	CCDL	1.60E-06	3.57E-05	7.91E-03	2.82E-07	
104	TLA	5.40E-06	1.99E-05	2.89E-02	5.76E-07	
105	CGV	8.20E-06	2.46E-05	4.29E-02	1.05E-06	
106	MV	6.60E-06	2.46E-05	3.45E-02	8.49E-07	
107	T2	3.80E-06	1.92E-05	2.04E-02	3.93E-07	
108	4 SUMS	9.00E-07	1.37E-05	4.99E-03	6.84E-08	
109	P3	1.10E-05	2.28E-05	5.81E-02	1.32E-06	
110						
111				SUM	SUM	
112				3.74E-01	8.34E-06	1.174E-05

Figure 13A shows a plot of the Table 1 data for the LOTC rate as a function of the time-since-fault, repair time for long time faults, T_{LT} . The short time repair interval in this analysis is fixed at 250 hours. This 250-hour repair time is also a time-since-fault repair time.

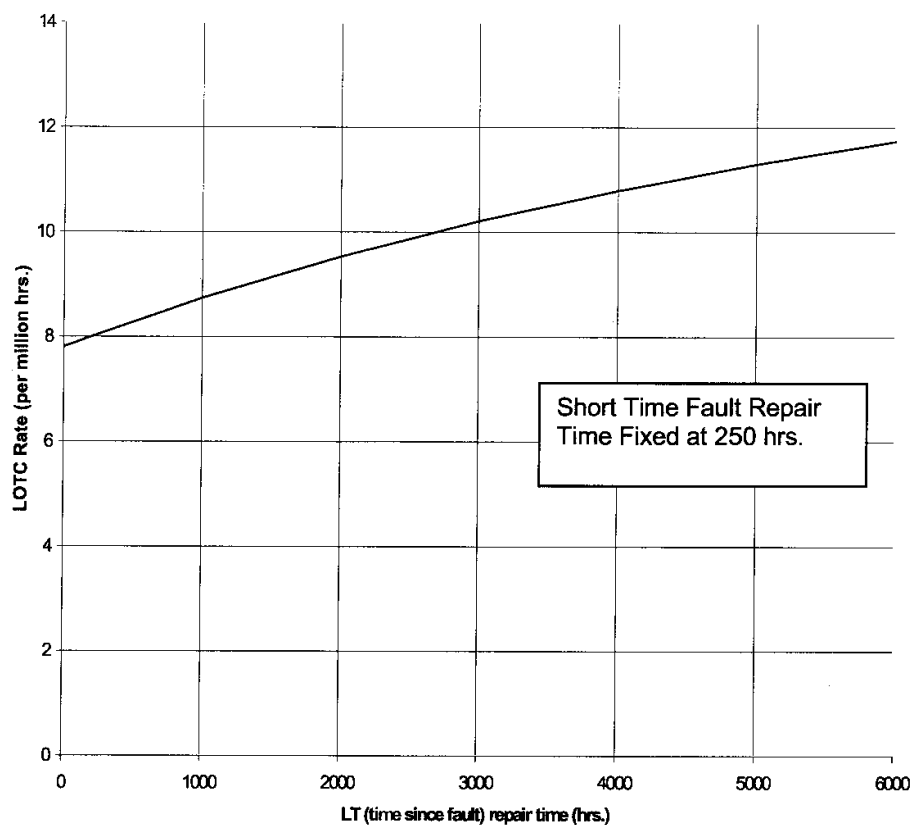


Figure 13A - LOTC rate (Table 1 data using Equation 20) as a function of the LT fault repair time for simple FADEC system example of Figure 12

The 10 per million LOTC rate (for engines installed on transport category aircraft) is achieved by repairing ST fault within 250 hours of their occurrence and LT faults within approximately 2700 hours of their occurrence. If this is an initial application of a FADEC system, the FAA's policy letter for LOTC analyses requires a 2:1 margin in the repair times simulation, with a maximum time-since-fault repair time of 125 hours for ST faults and 250 hours for LT faults. Thus, if this were an initial FADEC system application, those would be the maximum allowed limits, even though the analysis shows that a longer than 250-hour LT repair time would yield an LOTC rate less than 10 per million hours.

Figure 13B shows a comparison of the LOTC solution results (Table 1) for the Figure 12 Markov model using the complete single state Markov model equation (Equation 20) along with the first order approximation Equation 20c and the simplified solution equation given by Equation 20f.

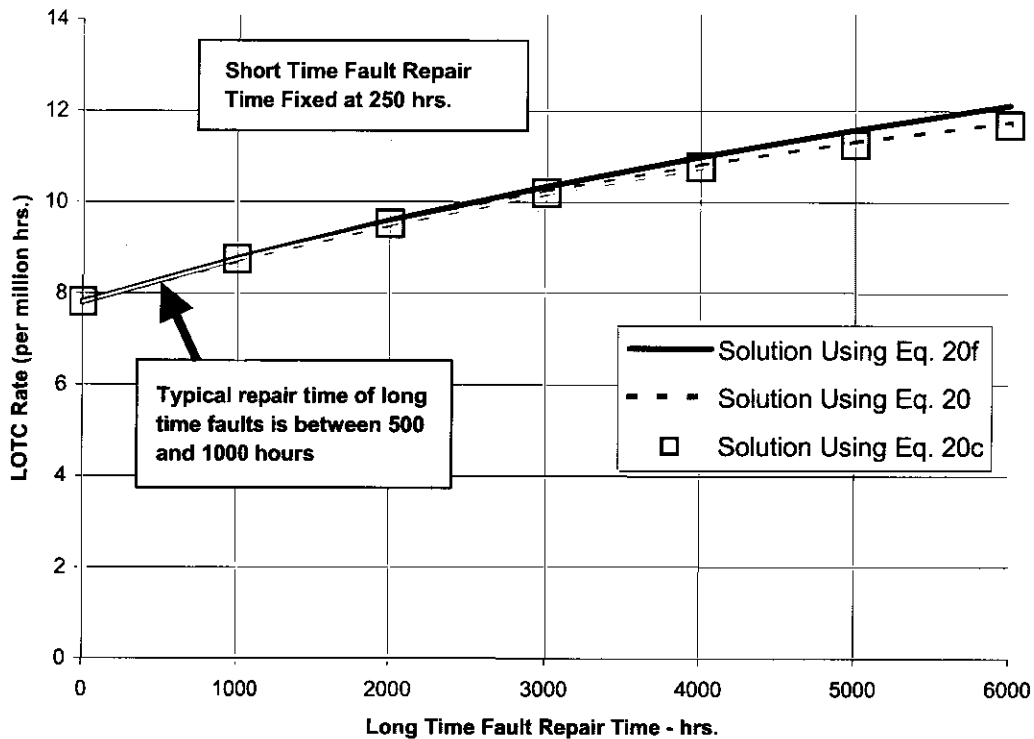


Figure 13B - Comparison of Figure 12 Markov model LOTC calculations Using Equations 20, 20c, and 20f

Figure 13

Table 2 shows a spread sheet of the calculations involved in determining the coefficients; a_0 , a_1 , b_0 , b_1 , c_0 , c_1 , d_0 , and d_1 , which are used in Equation 20c. Note how easy it is to calculate the coefficients, and the coefficients only have to be calculated once for the ST and LT fault states. This is much easier than doing the spread sheet layout of Table 1, and the first order approximation provided by Equation 20c is in excellent agreement with the more complex solution given by Equation 20 (and Table 1).

Table 3 - Spread sheet showing the calculations for determining the coefficients a_0 , a_1 , b_0 , b_1 , c_0 , c_1 , d_0 , and d_1 used in Equation 20c

	λ_{STi}	$\lambda_{STi-LOTc}$	$\lambda_{STi} * \lambda_{STi-LOTc}$	$\lambda_{STi} * \lambda_{STi-LOTc}^2$
ECU	1.77E-05	5.20E-05	9.20E-10	4.79E-14
PMA	1.50E-06	5.18E-05	7.77E-11	4.02E-15
	SUM		SUM	SUM
	$b_0 =$		$a_0 = b_1 =$	$a_1 =$
	1.92E-05		9.98E-10	5.19E-14
	λ_{LTi}	$\lambda_{LTi-LOTc}$	$\lambda_{LTi} * \lambda_{LTi-LOTc}$	$\lambda_{LTi} * \lambda_{LTi-LOTc}^2$
SBVA,B,C	2.22E-05	2.09E-05	4.64E-10	9.70E-15
PS	1.10E-05	2.28E-05	2.51E-10	5.72E-15
CCDL	1.60E-06	3.57E-05	5.71E-11	2.04E-15
TLA	5.40E-06	1.99E-05	1.07E-10	2.14E-15
CGV	8.20E-06	2.46E-05	2.02E-10	4.96E-15
MV	6.60E-06	2.46E-05	1.62E-10	3.99E-15
T2	3.80E-06	1.92E-05	7.30E-11	1.40E-15
4 SUMS	9.00E-07	1.37E-05	1.23E-11	1.69E-16
P3	1.10E-05	2.28E-05	2.51E-10	5.72E-15
	SUM		SUM	SUM
	$d_0 =$		$c_0 = d_1 =$	$c_1 =$
	7.07E-05		1.58E-09	3.58E-14

When the repair rates are high with respect to the failure rates into and out of the single fault states, the use of Equation 20f is certainly adequate.

High repair rates mean short repair times. Equation 20f is much simpler to use than Equation 20 because it only requires a one-time calculation of the terms:

$$\sum(\lambda_{STi}), \sum(\lambda_{LTi}), \sum(\lambda_{STi} * \lambda_{STi-LOTc+HM+UC}), \text{ and } \sum(\lambda_{LTi} * \lambda_{LTi-LOTc+HM+UC}).$$

The use of Equation 20c only requires two more terms to be calculated in addition to the above. They are:

$$\sum(\lambda_{STi} * (\lambda_{STi-LOTc+HM+UC})^2), \text{ and } \sum(\lambda_{LTi} * (\lambda_{LTi-LOTc+HM+UC})^2).$$

When the repair times are relatively short, such that the repair rates (i.e., the reciprocal of the repair times) are approximately 10 time or greater than the failure rates into and out of the various fault states, the use of Equation 20f should be adequate. From its ease of use and accuracy, Equation 20c is preferred.

7.4.2 Validity of the Calculated Data

As discussed in 7.2.4, single state Markov models are representative of a system when the repair rates for the states are frequent with respect to the failure rates into and out of the states. Having a frequent repair rate simply reduces the probability of having a second ST or LT fault occur during the time period that a ST or LT fault is allowed to exist. It is suggested that the repair time be at least 10 times greater than the highest of the failure rates into or out of all states in a given (i.e., ST or LT) group.

The highest failure rate for LT faults is the failure rate out of the CCDL fault state, which is 35.7×10^{-6} failures per hour. Using this number, the repair rate for all LT faults states should be no less than 35.7×10^{-6} units per hour. This equates to a repair interval, which is the reciprocal of repair rate, of 2800 hours. Hence, the data shown in Figure 13 for the LOTC rate of the system is increasingly inaccurate for LT repair times greater than 2800 hours. In this particular model, the highest failure rate of 35.7 per million hours is a bit less important because the failure rate into the CCDL state is only 1.6 per million hours; therefore, this state does not contribute significantly to the LOTC rate and it is unlikely to have this failure coupled with another LT fault in the 2800 hour period. The next highest failure rate is 24.6 failures per million hours and occurs from both the "CGV TM or LVDT" and "MV TM or LVDT" states. Multiplying this by 10 and taking the reciprocal yields a maximum repair time of 4064 hours. The model is reasonably accurate up to this time period.

In summary, although data is calculated and shown in Figure 13 for LT repair times up to 6000 hours, the data beyond 4000 hours is increasingly inaccurate in this particular single state model. Most FADEC system LT repair times are 1000 hours or less, and for these shorter repair times, a single state MM is usually quite adequate.

7.5 Second Example: A Single and Dual State Model of a FADEC System

A major engine manufacturer provided this second example. Without showing all of the failure rates and the particular failure states, Figure 14 shows a second example of a single state Markov model of a typical FADEC system. State #1 is the full-up state, states 2 through 24 are the single failure states, and state 300 is the LOTC state. Dual failure states, which are combinations of the single states, were added to the model, as shown in Figure 15. The dual states are numbered from 30 to 209, so there are 180 dual states represented. In both models, there are only three short time (ST) states. They are states numbered 2, 3, and 4. Using a fixed ST repair interval of 250 hours for these three states, the LOTC rates for both the single and dual state models are shown in Figure 16 as a function of the LT fault repair time. Note that at an LT repair time of 2000 hours, which is a long LT repair time, the single and dual state models only differ by about 3%, and at an LT repair time of 1000 hours, the two differ by less than 1%. This is an example which shows how small the contribution of the dual states is to the estimated LOTC rate.

7.6 Discussion of Markov Model and TWA Approaches, and the Use of Fault Trees (for Determining LOTC Rates When Operating with Faults)

As stated above, in comparing the MM approach with the TWA approach, the MM approach has the advantage of being able to balance the various states of a redundant system slightly better than the TWA approach. The use of Equation 20c allows an accurate MM result to be determined in a simple manner (i.e., the coefficients only have to be calculated once. See Table 2). Using the definitions for the fractional coefficients given by Equations 6 in this revised ARP significantly improves the "balancing" of the TWA approach. The TWA approach, with either the original fraction coefficients or the new defined ones, yields a conservative answer for the LOTC rate and is an acceptable method for completing the LOTC TLD analysis.

The use of fault trees to calculate the average failure rates of the system when operating with faults is quite acceptable, but the fault tree of the system needs to be completed with considerable care. Markov models tend to be a functional representation of the system. Fault trees tend to be more of a hardware representation of the system. For example, assume that one channel is operating with one thrust level angle (TLA) signal failed. Whether control remains in that channel or not, the only next failures that would cause the system to go to the LOTC state is the loss of the other channels CPU, power supply, or remaining TRA signal. (If control remains in the channel with the failed TLA signal and the cross-talk bus, which contains the remaining TLA signal, fails, the control can simply revert to the good TLA signal channel.) There have been examples of very complex fault tree models which calculated a very incorrect failure rate for this simple situation. Hence, if fault trees are used to calculate the failure rates of the system when operating with faults, do simple reasonableness checks on the results to see if they agree with what is logical. This is reasonable easy to do in a single state model.

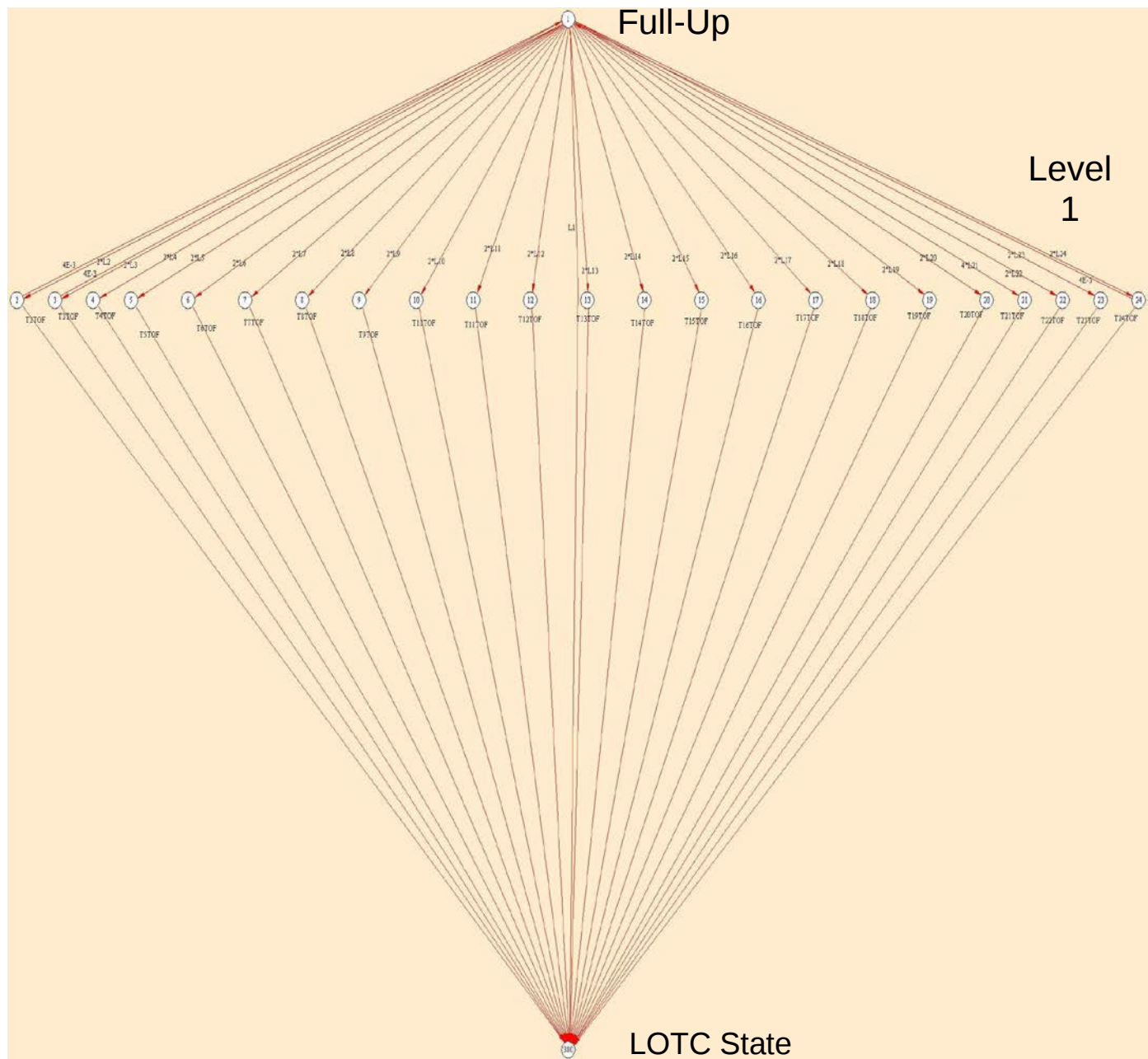


Figure 14 - Second example of single state Markov model of a typical FADEC system, with 23 single fault states

Cross-channel resource-

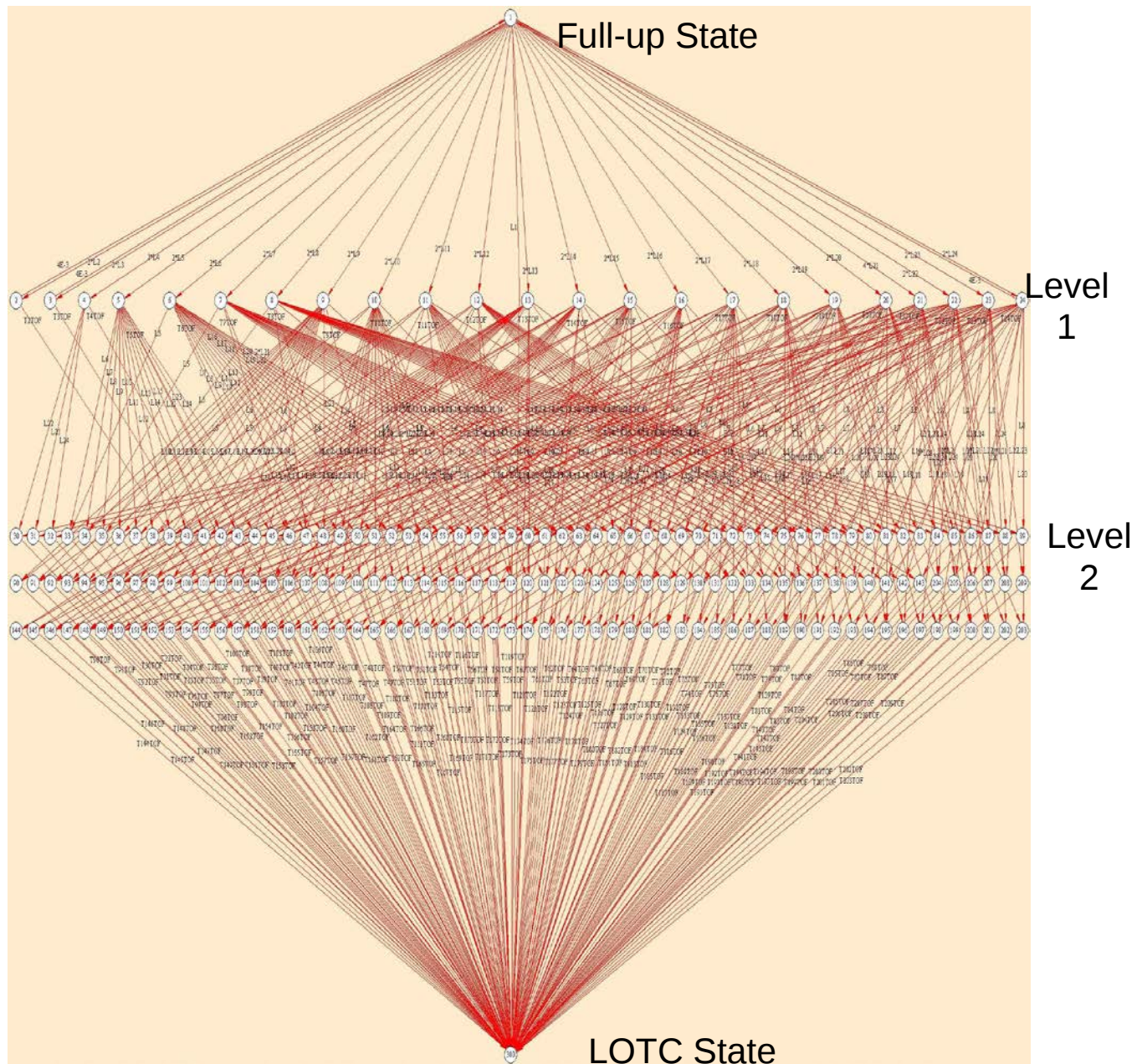


Figure 15 - Figure 14 model with 180 dual states added

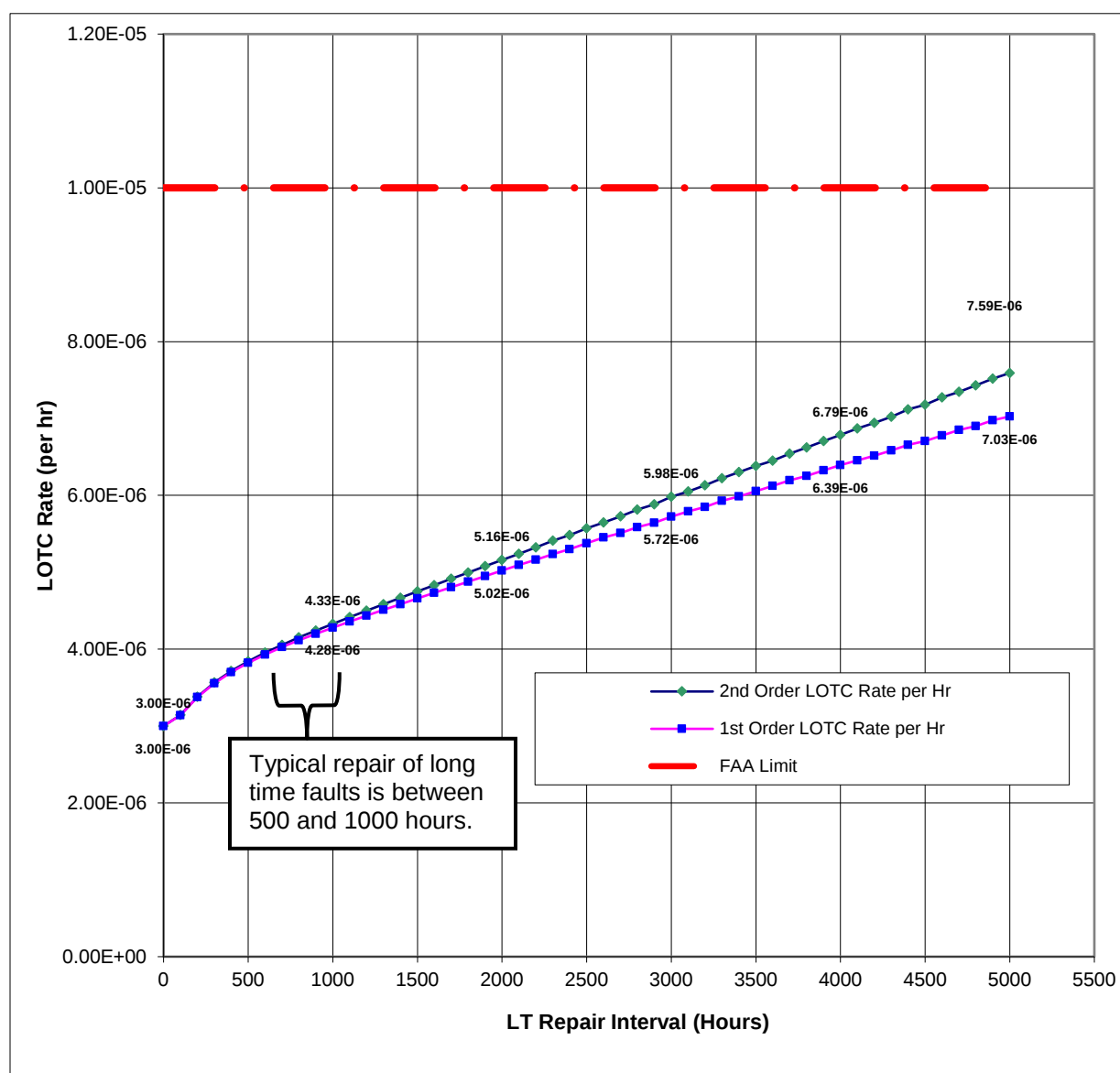


Figure 16 - LOTC rates as a function of LT repair time for both the single and dual state models of Figures 14 and 15

7.7 Time-Since-Fault (i.e., On-Condition) Repair Versus Periodic Inspection and Repair

In all of the above discussion, the repair intervals for ST and LT faults are based on time-since-fault repair. (This is also referred to as “On Condition” repair. The two nomenclatures are herein considered synonymous.) In this maintenance approach, a “clock” is started when the fault occurs, and after a certain number of hours have elapsed - like 100 hours for ST faults - the fault is repaired. This maintenance approach can be employed when the aircraft operator maintenance is immediately notified or aware of the occurrence of a fault. This works reasonably well for ST faults, because there is (generally) an aircraft “flight deck indication” presented to the flight crew of an ST fault condition, and maintenance can “start the clock” and track the fault to see that it is repaired within the required period. LT faults, however, are generally handled in a different manner. Most airframe operators do not wish to have a “flight deck indication” for something that is allowed to be in existence for 500 hours or more. Hence, LT faults are generally handled via an Periodic Inspection/Maintenance activity. This activity involves a periodic inspection of the FADEC system for LT type faults, and if LT faults are found, they must be repaired.

If an inspection and repair activity is used to implement fault maintenance, the inspection/repair interval should not be greater than twice the on-condition, time-since-fault time limit. This is because the fault could have occurred at any time during the interval, and "on average" the fault will have occurred half way through the interval. Hence, the fault has been "On Condition" for approximately $\frac{1}{2}$ the interval. This is true when the inspection interval is short with respect to the mean-time-between-failure (MTBF) of the sum of the items in the fault group.

The following presents a derivation for determining the periodic inspection interval time as a function of the time-since-fault repair time and the MTBF of the sum of the items grouped in the LT repair category.

The average time-since-fault, T_{TSF} , that a fault has been present (if found at inspection) is given by the following expression:

$$T_{TSF} = T_{Inspect} - T_{Mean-LT} \quad (\text{Eq. 21})$$

where:

$T_{Inspect}$ is the length of time between periodic inspections in hours.

$T_{Mean-LT}$ is the mean time in hours (from the start of the interval) where a LT fault is expected to occur.

$T_{Mean-LT}$ is evaluated as:

$$T_{MEAN-LT} = \frac{\int (t * e^{-\lambda(LTT)t}) dt}{\int (e^{-\lambda(LTT)t}) dt} \quad (\text{Eq. 22})$$

The integrations are from $t = 0$ to $T_{Inspect}$, and again, the term $\lambda(LTT)$ represents the total sum of all long term (i.e., LT) faults in both channels.

Completing the Equation 22 integration, substituting the result for $T_{Mean-LT}$ into Equation 21, and simplifying yields:

$$\frac{T_{TSF}}{T_{Inspect}} = \frac{1 - (1 - e^{-R})/R}{1 - e^{-R}} \quad (\text{Eq. 23})$$

where:

$$R = T_{Inspect}/T_{MTBF(LTT)}$$

$$T_{MTBF(LT)} = 1/(\lambda_{LTT})$$

This can be solved iteratively to obtain values for $(T_{Inspect}/T_{TSF})$ as a function of $(T_{TSF}/T_{MTBF(LT)})$. The results are shown in Figure 17. Note from this figure that if the value for the time-since-fault repair time is greater than approximately one-tenth the MTBF of the LT fault group (i.e., values greater than 0.1 on the "x" axis in Figure 17), the approximation of having the periodic inspection interval time be twice the time-since-fault repair time becomes increasingly inaccurate.

As shown in the derivation given in Figure 18, for $(T_{Inspect}/T_{MTBF})$ less than 2.0, a good approximation to Equation 23 is:

$$\frac{T_{TSF}}{T_{Inspect}} \gg 1/2 + (1/12) * (T_{Inspect}/T_{MTBF(LT)}) \quad (\text{Eq. 24})$$

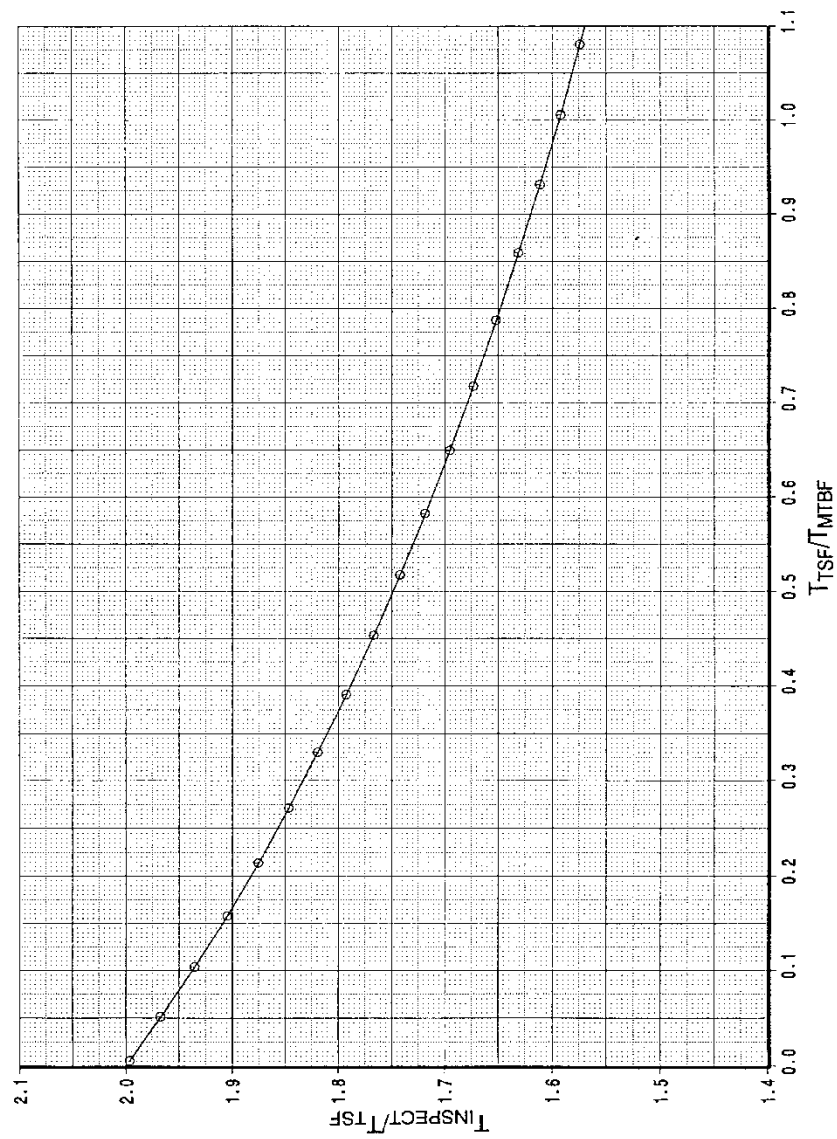


Figure 17 - ($T_{INSPECT}/T_{TSF}$) versus ($T_{TSF}/T_{MTB(LT)}$)

Using the Maclaurin series expansion for e^{-R} of

$$e^{-R} = 1 - R + R^2/2! - R^3/3! + R^4/4! + \dots$$

$$\frac{R - (1 - e^{-R})}{R(1 - e^{-R})} \approx \frac{R^2/2! - R^3/3! + R^4/4! + \dots}{R(R - R^2/2! + R^3/3! - R^4/4! + \dots)}$$

Dividing through by R^2 simplifies this to:

$$\frac{R - (1 - e^{-R})}{R(1 - e^{-R})} \approx \frac{1/2! - R/3! + R^2/4! + \dots}{1 - R/2! + R^2/3! - R^3/4! + \dots}$$

Dividing the right-hand side numerator by the denominator yields

$$\frac{R - (1 - e^{-R})}{R(1 - e^{-R})} \approx 1/2 + R/12 - R^3/720 + R^5/30240 - R^7/1209600 + \dots$$

For R less than approximately 2.0, the above is simplified to

$$\frac{R - (1 - e^{-R})}{R(1 - e^{-R})} \approx 1/2 + R/12$$

Inserting this approximation into Equation 23 yields

$$\frac{T_{TSF}}{T_{Inspect}} \approx 1/2 + T_{Inspect} / (12 * T_{MTBF(LT)})$$

This is Equation 24.

Figure 18 - Derivation of approximation given in Equation 24

Solving Equation 24 for $T_{Inspect}$ as a function of T_{TSF} and $T_{MTBF(LT)}$ yields:

$$\frac{T_{Inspect}}{T_{MTBF(LT)}} \gg 3 * \{-1 + [1 + (4/3) * (T_{TSF} / T_{MTBF})]^{0.5}\} \quad (\text{Eq. 25})$$

As in the above examples, most reliability tools are constructed to analyze systems with faults being repaired on a time-since-fault basis. Hence, having determined T_{TSF} from the analysis, the inspection interval corresponding to that T_{TSF} is determined from Figure 15 (or, if applicable, Equation 25).

For example, if there are 10 faults in the long term (LT) category and the failure rate for each is 20×10^{-6} failures/hour, the total LT failure rate would be 200×10^{-6} failures/hour, and the T_{MTBF} for the group would be 5000 hours. If a reliability analysis yields the result that the maximum on-condition operational time for an LT should be limited to 3000 hours, Equation 29 can be used to calculate a corresponding inspection interval of 5125 hours - which is significantly less than twice the "on condition" repair interval of 3000 hours. In this case, the time-since-fault or "on condition" length of time that an LT fault is allowed to exist (before requiring repair) is long in comparison to the expected time, $T_{MTBF(LT)}$, of a LT fault; therefore, the approximation of using twice the calculated T_{TSF} interval as the periodic inspection interval would not be a good one (see Figure 15).

8. CALCULATION APPROACHES - DUAL ENGINE ANALYSIS

8.1 Time-Averaging Approach

The dual engine LOTC rate analysis is not significantly different than the single engine analysis. The "average" dual LOTC rate is given as:

$$\lambda_{DUAL-ENG-LOTC-AVE} = \frac{2 \cdot T_{DIV} \cdot (T_{FL} - T_{DIV}) \cdot (\lambda_{LOTC-AVE})^2}{T_{FL}} \quad (\text{Eq. 26})$$

where:

T_{FL} is the flight length

T_{DIV} is the diversion time on one engine

For the equation to be valid, (T_{DIV}/T_{FL}) must be less than 0.5

(A derivation of Equation 26 is given in Appendix E.)

Using an average λ_{LOTC} of 10^{-5} per hour, T_{FL} as 4.5 hours, and T_{DIV} as 1 hour, the dual engine LOTC rate is calculated as:

$$\begin{aligned} \lambda_{DUAL-ENG-LOTC-AVE} &= \{2 \cdot 1 \cdot (4.5 - 1) \cdot (10^{-5})^2\} / 4.5 \\ &= 0.155 \cdot 10^{-9} \text{ events per flight hour} \end{aligned} \quad (\text{Eq. 27})$$

The reason that the result is small is that the twin-engine aircraft does not proceed to destination after the first engine failure. It diverts to the nearest suitable airport. Hence, the exposure time for the second engine failure is limited. If an extended operations (ETOPS) scenario is simulated, T_{FL} could be up to 16 hours and T_{DIV} is approximately 3 hours.

In this case:

$$\begin{aligned} \lambda_{DUAL-ENG-LOTC-AVE} &= \{2 \cdot 3 \cdot (16 - 3) \cdot (10^{-5})^2\} / 16 \\ &= 0.488 \cdot 10^{-9} \text{ events per flight hour} \end{aligned}$$

Hence, using an average engine control system failure rate of $10 \cdot 10^{-6}$ is consistent with meeting the FAR/CS 25.1309 requirement for meeting a 10^{-9} per hour failure rate for a dual engine failure event (caused by control system failures).

8.2 Maximum Specific Risk Failure Rates as a Function of Dispatch Configuration

The probability of a dual engine LOTC event during any given flight is generally termed "the specific risk" of that flight. Since the FADEC control systems for each engine are independent of each other, the specific risks for a twin-engine aircraft are calculated from:

$$\lambda_{DUAL-ENG-LOTC-AVE} = \frac{2 \cdot T_{DIV} \cdot (T_{FL} - T_{DIV}) \cdot \lambda_{SPEC-LOTC-ENG\#1} \cdot \lambda_{SPEC-LOTC-ENG\#2}}{T_{FL}} \quad (\text{Eq. 28})$$

Using a full-up to LOTC fault rate of 6×10^{-6} for the mechanical/hydromechanical elements plus the undetected faults, and the maximum allowed ST- and LT-to-LOTC rates of 100×10^{-6} and 75×10^{-6} respectively (these values include the hydromechanical and undetected faults), the specific "worse case" dual engine LOTC rates for the various dispatch states for a flight of 4.5 hours with a 1-hour diversion are shown in Table 3.

Table 4 - Dual engine specific risk as a function of dispatch configuration

Dispatch States (eng1/eng2)	Dual LOTC Rate (failures/hour)
Full up/Full up	0.056×10^{-9}
Full up/ST	0.933×10^{-9}
Full up/LT	0.700×10^{-9}
LT/LT	8.750×10^{-9}
ST/LT	11.667×10^{-9}
ST/ST	15.556×10^{-9}

The above calculations assume that the engine control systems on the two engines are in the fault condition state listed in the table at dispatch.

Dispatches of configurations with dual engine LOTC rates greater than 10^{-9} failures per hour are allowed by the FAA, but only for limited periods of time. Any dispatch allowance should be determined via discussions with the FAA concerning the specific configurations and the integrity of the FADEC system(s) when operating in those configurations.

9. SUMMARY

The concept of Time Limited Dispatch (TLD) for FADEC systems has worked well in service. Prior to the release of the FAA's Engine and Propeller Directorate policy letter governing certification of FADEC systems, there were no FAA "rules" or "guidelines" governing dispatch of redundant systems in non-full-up configurations, and even though many systems on modern day commercial transports are using electronic redundancy, the FADEC system is still the only one (currently) employing the use of TLD. The approach has provided engineering guidance to maintenance and dispatch policies.

The MM approach appears to be the better approach to analyzing FADEC systems. It's flexible and reasonably easy to use. The capability to implement and easily change "transition paths" and rates, as well as repair intervals, is a distinct advantage. The first order differential equations are easily solved.

Two items should be recognized when using TLD:

- Maintenance becomes a certification item. The airline operators do not like this. They do not like maintenance, which is traditionally an FAA field operations Part 121 issue, to be controlled by an FAA Engine or Aircraft certification group (see Appendix D for more discussion).
- It brings to the "front" the issue of dispatching systems (for limited periods of time) in configurations where the specific risk of a catastrophic event on a given flight may be greater than 10^{-9} failures per hour.

The first of these tends to be a "political issue." There isn't much the aircraft or engine manufacturers can do to help this situation. FAA aircraft certification groups associated with finding compliance with 14 CFR Parts 23, 25, 27, 29, and 33 and the Flight Standards groups associated with Part 121 operations will both be involved in "certification" and "operations" decisions, and trying to draw a distinct line between the two areas will become increasingly difficult. FADEC redundancy is not simply provided for economic purposes. It's there for integrity also. This needs to be recognized.

The second item is always controversial; however, the use of "fleet averages" to show compliance with the FAA FAR 25.1309 Systems and Equipment requirement (that failures which lead to catastrophic events be "extremely improbable") has been accepted by the FAA Transport Airplane Directorate (Part 25).

10. NOTES

10.1 Revision Indicator

A change bar (|) located in the left margin is for the convenience of the user in locating areas where technical revisions, not editorial changes, have been made to the previous issue of this document. An (R) symbol to the left of the document title indicates a complete revision of the document, including technical revisions. Change bars and (R) are not used in original publications, nor in documents that contain editorial changes only.

PREPARED BY SAE COMMITTEE E-36, ELECTRONIC ENGINE CONTROLS

APPENDIX A - EARLY APPLICATIONS

A.1 EARLY ELECTRONIC APPLICATIONS

For the most part, early turbine engine powered aircraft used hydromechanical controls. There were electronic systems on early turbine engine applications, but generally they were limited to simple functions, such as rotor speed limiters and prop speed synchronizers. In most cases, these were single channel, analog-type systems. Since the engine had a "full" hydromechanical control system as basic equipment, the FAA generally allowed the aircraft to be dispatched for a period of time with the electronically controlled function(s) inoperative. An example of such a case was the electronic fan speed limiter used on the Rolls Royce RB211 engine used on the Boeing 747 and Lockheed L-1011 aircraft. The FAA generally determined the "allowable" dispatch interval based on the importance of the function. In the case of the RR limiter, the function was considered to be relatively important, and therefore, the FAA limited the "electronics inoperative" time to 25 hours.

A.1.1 Supervisory Engine Controls

The use of electronics widened as the engines became more complex to control and an improved interface with the engines (by the flight crew) was desired. This led to the use of what were termed "supervisory controls." These control systems employed much more electronics to achieve the desired control/interface functions, but they still generally employed a "full" hydromechanical controller for backup. The electronic supervisory controls were constructed in both analog and digital versions. Examples were the electronics used on the PW JT9D, GE CF6-80A/-80C2, GE- SNECMA CFM 56-2/-3, and RR RB211-535 engines. Although the hydromechanical controllers on these engines generally contained all of the functions needed to operate the engines, the aircraft on which they were installed began using signals from the supervisory electronics portion of the control to achieve improved engine/aircraft integration and operation during "electronic system" operation. For example, auto throttle operation was significantly simplified and improved during electronic engine controller operation, and the increase in crew work load in two-crew cockpits was always a discussion issue when the engine electronics were inoperative. Hence, the "allowable" time period of electronics inoperative operation always received considerable discussion. In (approximately) 1982, the FAA instituted a policy change that required most items affecting basic aircraft operation/crew interfaces to be repaired within 10 days. The supervisory electronic controls were considered to be in this category; therefore, the aircraft manufacturer's master minimum equipment list (MMEL), which is the FAA approved document controlling maximum allowable non-full-up dispatch operations, contains this time limitation.

A.1.2 FADEC Engine Controls

As the commercial transport turbine engines became more complex, it became apparent that the hydromechanical controllers were becoming incapable of providing all of the desired functions as well as the "full time" (i.e., electronics always operative) interface desired by the crew. Hence, FADEC engine controllers were developed by the engine manufacturers. These were dual channel electronic control systems that provided complete engine operation and the desired crew interface, even with one channel inoperative. It was anticipated that the dual-channel architecture would achieve excellent engine control system integrity. However, when the first engine, the PW 2037, with such a system was certified on the Boeing 757 aircraft, there were no guidelines in place to allow operation with faults in the electronic portions of the control. Lacking guidelines, the FAA took the very conservative approach of allowing the aircraft to be dispatched with faults in only one of the channels of one engine. In addition, the FAA did not allow the aircraft to leave a station where "repairs could be made." Hence, the aircraft was not allowed to dispatch with engine controller faults if there was a "spare" controller available at that station. This limitation on aircraft dispatchability is a concern to the airline operators.

APPENDIX B - DISCUSSION OF SOME TYPICAL FADEC SYSTEM FAULTS AND THEIR APPLICABILITY TO THE LOTC ANALYSIS

B.1 DISPLAY PARAMETERS PROCESSED BY THE CONTROL

There are various faults that affect aircraft dispatch, but have no effect on the engine control's LOTC rate. An example of such a fault is loss of exhaust gas temperature (EGT) or inter-turbine temperature (ITT). Turbine-powered engines are required to have an operative gas temperature display at dispatch. Hence, the aircraft is not dispatchable without one, but since (generally) loss of gas temperature indication has no effect on the LOTC rate of the control and loss of gas temperature in-flight should not cause the engine to be manually shut down (as verified by the engine manufacturer's operating instructions), the loss of gas temperature would not have to be considered in the analysis, even though the control might be processing the gas temperature parameter for display purposes.

NOTE: If the control has failures that cause EGT to read high, those failures need to be included in the LOTC analysis, because a high EGT reading could definitely lead to a crew-initiated in-flight shutdown of the engine. Cockpit displays of other engine display parameters being processed by the control system are in this same category as long as they do not affect the control's LOTC rate or cause the crew to shut down the engine.

B.2 DISPLAY OR OTHER PARAMETERS AFFECTING CONTROLLER OPERATION

Examples of display or other parameters that may affect controller operation are rotor speeds. In the case where the primary thrust display is engine pressure ratio (EPR), it has generally been acceptable to dispatch the aircraft with a rotor speed display on one engine inoperative provided all of the other parameter displays are operative. However, if that parameter is also unavailable to the control, and the control needs that parameter to implement "normal" operation of the engine, the engine control should be considered non-dispatchable without the parameter UNLESS engine operation has been demonstrated and certified by the FAA in that configuration. Hence, even though the control may synthesize the unavailable parameter in an effort to avoid a LOTC event from occurring, the control should not be dispatched without the parameter unless full engine operation has been certified in that configuration. In these cases, loss of the parameter to the control should be assumed to result in a LOTC event.

B.3 AIRCRAFT PARAMETERS USED BY THE CONTROL

It is generally the case that during normal operation the engine control will receive and use various aircraft signals in implementing its control function. Examples of the signals might be the aircraft air data signals. Since these signals may affect the operation of all engines, the control system should be configured to detect failures and undetected soft shifts in these signals so that an unacceptable thrust change on all engines is avoided and the engines are not placed outside of their certified operating envelope. (The FAA Part 25 requirement is that the failure of aircraft signals common to all engine controls shall not result in a thrust loss of more than 2% in the takeoff envelope.) This being the case, it can generally be assumed that loss of these aircraft signals does not have to be included in the engine controls LOTC analysis. There is an exception to this: if the aircraft signals are used to "validate" the engine controller's own dedicated signals, then loss of the aircraft signals may leave the controller in an instantaneously higher LOTC rate, and they should be included in the analysis. For example, on EPR-controlled engines the dedicated engine controller total pressure signal, PT2, may be validated using the aircraft's air data total pressure signal. If this is the case, then loss of air data information - although not directly causing a LOTC event - may leave the controller in an instantaneously higher LOTC rate configuration because a soft shift in engine PT2 may not be detectable and could lead to a greater than 10% thrust loss event. If this is the case, then loss of aircraft signals, such as air data, should be contained in the engine controller's LOTC analysis because they would affect the probability of a LOTC event.

B.4 BACKUP ELECTRICAL POWER

Another area similar to the above is backup electrical power. Although the current FAA (Part 33) requirement is that each engine's FADEC have a dedicated power supply which is independent from aircraft power, many FADEC applications use aircraft electrical power as a backup power source. The question arises as to whether the use of aircraft backup power can be used in the engine controller's LOTC analysis to avoid a LOTC event when the dedicated power supply fails. In many ways, it certainly seems reasonable. However, aircraft power is subject to interrupts, and since the engine manufacturers (generally) have not chosen to demonstrate proper and acceptable FADEC controller and engine operation during such interrupts, the approach taken has been to assume that those interrupts will result in an engine LOTC event. Hence, credit for the use of backup power has (generally) not been sought in certification, and the use of back-up power has not been included in the LOTC analysis. (A related approach would be to assume a LOTC event occurs on a power interrupt, and put a number into the analysis for the probability of a power interrupt event. However, validating that number is a difficult thing to do, so this approach is not often used.)

Although not taking certification credit for back-up power, all FADEC systems using it have gotten field credit for it. There have been numerous FADEC dedicated alternator failures in the field, and in the vast majority of those events, the control system operated properly on back-up power and no LOTC or inflight shutdown (IFSD) event occurred or was recorded. This is one of the reasons why the field service numbers for engine control system caused LOTC events are considerably less than our analysis predictions.

APPENDIX C - DISCUSSION OF THE MMEL, DDG, CMRS, AND THEIR RELATIONSHIP TO FADEC SYSTEM MAINTENANCE (THE HANDLING OF ND, ST, AND LT FAULTS)

C.1 DEFINITIONS

C.1.1 MMEL Items and CMRs

The MMEL is the aircraft's master minimum equipment list. The name is a bit of a misnomer, as it is a list of the equipment that is allowed to be inoperative at dispatch provided that (1) other equipment, (2) operational (i.e., flight crew) procedures, or (3) a maintenance activity (other than repairing the faulty item) is implemented for that flight. Each aircraft-type design has its own MMEL. It is a FAA (Part 121) approved document. The aircraft operators use this MMEL to prepare their own minimum equipment list (MEL) for their operations of that aircraft. The airline operators can be conservative and delete items (contained in the MMEL) when constructing their own MEL for that aircraft, but they cannot add items which are not covered in the aircraft manufacturer's MMEL. Each U.S. operator's MEL is also approved by the FAA.

The DDG is the aircraft manufacturer's dispatch deviation guide. It is an aircraft manufacturer's document which is not FAA approved. It is supplied to the customers to allow them to easily cross-correlate cockpit messages and other aircraft displays to the MMEL, with a description of any needed maintenance action, crew procedure, or performance penalty that need be employed for that dispatch. It contains a "re-type" of the FAA approved MMEL. An example might be a message like "ENG 1 TURB COOL" referring to a failure/fault in the turbine case cooling system on engine number one. The DDG would list the message (refer to MMEL ATA Chapter 73), where the MMEL would state: "Dispatch is allowed provided the appropriate fuel burn and maintenance actions are implemented," and the DDG would state what those are, such as planning for 0.5% greater fuel burn and locking the cooling valve closed prior to dispatch.

C.2 CMRS AND THE MRB REPORT

C.2.1 Certification Maintenance Requirements (CMRs)

The acronym CMR represents a certification maintenance requirement. This acronym is used to "highlight" a maintenance activity which must be performed on a system in order for the system to comply with its type design certification (reliability) requirements. The term CMR refers to a maintenance activity which has been submitted to the FAA Part 33 (or Part 25) certification office as part of the system's reliability analysis. Hence, it is part of the engine or aircraft manufacturer's certification documentation. CMRs are listed in a special section of the aircraft's maintenance planning document (MPD).

C.2.2 The Maintenance Steering Group and the MRB Report

The maintenance review board (MRB) is a group of airline, engine, and aircraft manufacturers, and other suppliers. They are people who review all of the systems on an aircraft and recommend, in an MRB report for that aircraft, the various maintenance activities for the aircraft systems and other elements of the aircraft, such as structures. This MRB activity generates "task cards" which describe the various recommended maintenance activities. Task cards for CMRs are also included in the MRB report. These tasks are entered into the aircraft's maintenance planning document (MPD). CMR tasks are placed in a special section of this document. Whereas all other maintenance tasks in the report are recommended activities, CMRs are required maintenance tasks, and the aircraft operators must maintain special paper work showing that they have complied with the CMR task descriptions. Since CMRs require specific maintenance tasks and special documentation, they are not well received by the operators.

C.3 DISPATCHABILITY AND THE MMEL

C.3.1 "No Dispatch" and Short Term (ST) Repair Items

The "No Dispatch" group of faults is obviously that: the FADEC system has suffered a fault which must be repaired prior to dispatch. This type of fault is displayed to the flight crew via a "message" or light on the main engine displays panel. Thus, the display is available to the flight crew following engine start. An example of such a fault is loss of a FADEC system's ambient pressure sensor(s). FADEC systems which need ambient pressure for proper engine control are considered non-dispatchable with loss of that dedicated signal. (The FADEC systems requiring ambient pressure for proper operation may also receive ambient pressure from the aircraft's air data system. If so, these systems would operate properly using that signal on a "get home" basis, but the systems are not certified to dispatch in that configuration.) No dispatch items are handled via the DDG and MMEL, which would indicate that when such a message appears, the fault associated with that message must be repaired prior to dispatch.

Items that should be repaired in the near future (i.e., short term items) are also handled via the DDG and MMEL. These documents would indicate that the item is allowed to be deferred for a given period of time before repair is required.

Short term items are noted by maintenance on at least a daily basis. In many cases, it may even be on a per flight basis. Generally, the indications for these faulty conditions may not be directly evident to the flight crew. The indications may be stored in a location that must be "dispositioned" by the aircraft's maintenance group before the aircraft is "released" to its operations group. In typical operations, the maintenance group would review this information, note the existing faults affecting dispatch, record and make disposition of any new ones using the DDG and MEL, note the new ones in the aircraft's maintenance log, release the aircraft for service, and schedule the appropriate repairs to be within the allowable MEL period.

Since short term faults are found by maintenance on almost an immediate basis, they have been termed "on condition" faults. Hence, the FADEC system reliability analysis should use the same time period for exposure to these faults as listed in the MMEL.

Theoretically, the short term repair requirement for FADEC system ST faults could also be classified as a CMR task and listed in the aircraft's MPD, because the need to perform the repair within a given time period would have been submitted to the FAA (Part 25 and Part 33) as part of the FADEC system's certification data package. However, MMEL items are generally not classified as CMRs or listed in the MRB report. The repair requirements for short term and LT faults are listed as "limitations" in the engine's and aircraft's Type Data Approval documentation. For ST faults, the repair requirement is passed through to the aircraft's master minimum equipment list (MMEL). The airlines aircraft operator is not free to extend the ST fault repair requirement without an appropriate change to the engine's and aircraft's type data certification documentation - which would require approval from the engine and aircraft certification offices.

C.3.2 Long Term (LT) Repair Items

Many FADEC system faults have a small effect on the instantaneous LOTC rate. Assuming that the fault does not (1) render one channel incapable of operation, or (2) result in an instantaneous LOTC rate greater than 75 per 10^6 hours of operation, it may be acceptable to allow a considerable period of time to elapse, such as 500 hours or more before repair, and still comply with the overall average LOTC rate of less than 10 failures per 10^6 hours of operation. These types of faults are generally termed "normal maintenance items." Faults of this type are generally stored in a location different than that discussed in D.3.1, because the aircraft's maintenance group does not want to have to "disposition" these faults on a daily or per-flight basis. The maintenance requirement is that this maintenance message location be reviewed periodically, the faults noted, and the appropriate repairs scheduled.

Since this periodic inspection and repair requirement is contained in certification documentation and is used to show compliance with the reliability requirements of the system, this task may be identified as a CMR by the FAA. If identified as such, the task would have to be listed in the CMR section of the MRB report and MPD. As stated above, operator activities relating to "the reporting" on CMR tasks (to the FAA) causes them additional expense; hence, CMR tasks are not well received by the operators. Traditionally, if a CMR task is not completed within the allocated time period, the aircraft is classified as "non-airworthy" and cannot be released for service until the task is completed. (The recent ANE FAA Policy Letter for Time Limited Dispatch allows a 50 hour extension of the LT fault inspection/repair time interval to accommodate unusual circumstances.)

C.4 OPTIONS FOR REMOVING LT FAULTS FROM CMR CLASSIFICATION

There are several options to pursue to remove LT faults from their CMR classification.

C.4.1 Put All Faults to the Short Term Interval

The first of these is to simply place all LOTC faults in the short term category and use the MMEL to handle their repair. This will cause the aircraft operator to perform maintenance sooner than necessary, but it eliminates the expense of reporting on CMR task items to the FAA. Some operators prefer this approach. This approach tends to be a hardship on operators which have a policy of not leaving a "home base repair station" with MMEL items.

C.4.2 Control Timers

A second approach might be to put "timers" into the FADEC system which starts a clock when "long term fault" occurs, displays a maintenance message for the fault, and when the clock indicates that there is approximately 100 to 150 hours to go before the fault needs repair, raise the level of the fault to the short term category. This would cause the fault to become immediately aware to maintenance via the MMEL, and its repair would be scheduled. This approach has the advantage of allowing maintenance to review the long term faults and take the appropriate maintenance action before the fault is raised to the MMEL level. The disadvantage is the extra software associated with the "timers," and some difficulties associated with those operators who change the FADEC controller - because it is one of the easier LRUs to change - when a system fault is indicated. The advantage of this is that it affords adequate time to repair the fault, after the initial maintenance message - before the fault is raised to the short term repair level. Also, since the software is certified by the FAA and cannot be changed without their approval, the FAA still controls the inspection interval.

C.4.3 Dual Long Term (DLT) Fault Category

Another approach might be to "save" the first long term fault in the EEC's memory device and await the occurrence of a second long term fault. When the second fault occurs, send an appropriate message to the aircraft which raises the level of required maintenance to the short term, MMEL, 10-day category. This is relatively simple to do in software, but it requires that all combinations of two long term faults not result in an instantaneous LOTC rate exceeding the 100 per million hour short term category upper limit and that repairing the multiple faults within 100 to 150 hours will be sufficient to meet the required 10 per million hour average LOTC rate. Provided the above requirements can be met, this approach is relatively straightforward and should work.

C.4.4 Life-Limited-Parts Section of Engine Maintenance Manual

The FAA has accepted that listing the inspection/repair requirements relating to FADEC system TLD operations in the "life limited parts" section of the engine maintenance manual is sufficient for ensuring "on time" maintenance, and that when this approach is used, no CMR is considered necessary. Limitations contained in the life limited parts section of the engine maintenance manual are FAA (engine certification office) approved and cannot be changed without FAA concurrence.

C.4.5 Messages for Other than LOTC-Related Events

The TLD No Dispatch and Short-Term Dispatch flight deck messages have historically been utilized to also indicate failures which are not associated with LOTC. This is done to limit the number of crew alerts and for convenience when the TLD dispatch category time limits are in line with the desired repair interval for the non-LOT related items. These non-LOT items can include both engine and aircraft signal failures. These items may be safety related, associated with the engine, or secondary aircraft systems.

C.4.6 Examples

Safety-related items include the loss of overspeed protection or degraded overspeed protection systems.

Secondary engine related items include fuel and oil filter delta pressure monitoring faults.

APPENDIX D - PROBABILITY OF A DUAL ENGINE FAILURE WITH DIVERSION AND TURNBACK

The following is a derivation of the probability of a dual-engine inflight failure taking into account turnback and diversion. Each engine is assumed to have an exponential failure rate λ . The planned flight duration is T hours. If at any point during the flight one of the engines fails, the airplane will either (1) return to its point of origin, (2) divert to an alternate landing site exactly D hours away, or (3) continue to its planned destination, whichever results in the earliest landing. For simplicity, we will assume that $\lambda \cdot t$ is small enough that $\lambda \cdot t \approx 1 - e^{-\lambda t}$.

The possibilities of dual engine failures can be divided into three cases, depending on when the first engine failure occurs. For each case, the probability of a dual engine failure can be directly computed by integrating the product of the probability density for the first failure times the corresponding probability that the second failure will occur prior to landing. Note that the rate associated with the first failure is 2λ (since either engine can fail), whereas the rate for the second engine failure is just λ .

Case 1: If the first engine failure occurs during the period from $t = 0$ to D , the airplane will return to its point of origin. Letting t denote the time of the first failure, the exposure to the second failure is the period from t to $2t$. Thus, letting τ denote the time of the second failure, the probability of dual engine failure in this case is as shown in Equation D1:

$$\Pr\{\text{case 1}\} = \int_0^D (2\lambda) \left[\int_t^{2t} (\lambda) d\tau \right] dt = \lambda^2 D^2 \quad (\text{Eq. D1})$$

Case 2: If the first engine failure occurs during the period from $t = D$ to $T-D$, then the airplane will divert to an alternate landing site exactly D hours away. Thus, the probability of dual engine failure for this case is as shown in Equation D2:

$$\Pr\{\text{case 2}\} = \int_0^{T-D} (2\lambda) \left[\int_t^{t+D} (\lambda) d\tau \right] dt = 2\lambda^2 D T - 4\lambda^2 D^2 \quad (\text{Eq. D2})$$

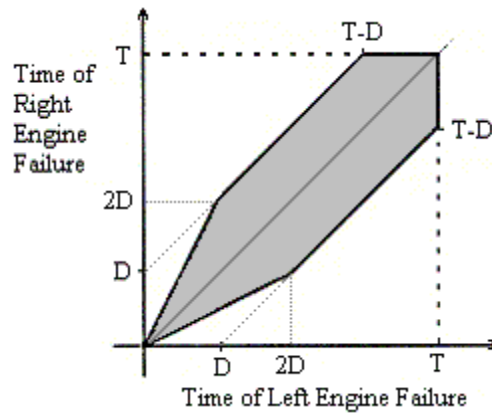
Case 3: If the first engine failure occurs during the period from $t = T-D$ to T , then the airplane will continue to its planned destination, so the probability of a dual engine failure for this case is as shown in Equation D3:

$$\Pr\{\text{case 3}\} = \int_{T-D}^T (2\lambda) \left[\int_t^T (\lambda) d\tau \right] dt = \lambda^2 D^2 \quad (\text{Eq. D3})$$

The total probability of dual engine failure is just the sum of the probabilities of these three cases:

$$\Pr\{\text{dual IFSD}\} = 2\lambda^2 D(T - D) \quad (\text{Eq. D4})$$

This result can also be deduced directly from a plot of operational hours of the left engine versus operational hours of the right engine as shown in Figure D1.

**Figure D1**

Beginning with both engines operational, each has a constant failure rate of λ during the next T hours, so the probability of both engines failing during this period is simply $\lambda^2 T^2$. This is represented by the area of the large square in the figure.

However, because of the turnback and diversion, only a fraction of these dual failures will occur during a single flight. Specifically, only those points that fall inside the shaded area correspond to dual failures on a single flight. Therefore, if we multiply $\lambda^2 T^2$ by the fraction of shaded area to total area inside the square, we will have the probability of dual engine failure during a single flight.

The two large outer triangles obviously have a combined area of $(T-D)^2$. This area represents the dual failures that are avoided due to diversion. The two smaller triangles have a combined area of D^2 , representing the dual failures that are avoided due to turnback. Therefore, the total probability of dual engine failure during a single flight is as shown in Equation D5:

$$\frac{T^2 - (T-D)^2 - D^2}{T^2} \lambda^2 T^2 = 2\lambda^2 D(T-D) \quad (\text{Eq. D5})$$

This is identical to the expression derived previously. To normalize this probability to a per-hour basis, we divide by the planned flight time T , which gives:

$$\text{Pr(dual failure)}_{\text{per hour}} = 2\lambda^2 (T-D)D/T \quad (\text{Eq. D6})$$

APPENDIX E - REVIEW OF THE COEFFICIENTS USED IN THE TIME-WEIGHTED-AVERAGE (TWA) EQUATION

This includes a discussion of:

1. The coefficients used in a single state Markov model, which maintains all of the single ST and LT states as separate states, and
2. The coefficients of a single state Markov model, which combines all ST and LT faults into a single (average) ST and LT state.

In the simple time-weighted-average (TWA) approach, the equation for the LOTC rate in 7.1 is given as:

$$\lambda_{\text{LOTC-AVE}} = \lambda_{\text{HM+UC}} + \lambda_{\text{FU-LOTC}} * \text{Fract}(\text{FU}) + \lambda_{\text{ST-LOTC-AVE}} * \text{Fract}(\text{ST}) + \lambda_{\text{LT-LOTC-AVE}} * \text{Fract}(\text{LT}) \quad (\text{Eq. E1})$$

where:

$$\lambda_{\text{HM+UC}} = \lambda_{\text{HMC}} + \lambda_{\text{UC}}$$

and λ_{HMC} , λ_{UC} , $\lambda_{\text{FU-LOTC}}$, λ_{STT} , λ_{LTT} , $\lambda_{\text{ST-LOTC-AVE}}$, $\lambda_{\text{LT-LOTC-AVE}}$, $\text{Fract}(\text{FU})$, $\text{Fract}(\text{ST})$, and $\text{Fract}(\text{LT})$ are all explained in the text of that section. The definitions for $\lambda_{\text{FU-LOTC}}$, λ_{STT} , λ_{LTT} , $\lambda_{\text{ST-LOTC-AVE}}$, $\lambda_{\text{LT-LOTC-AVE}}$ were given as:

$$\lambda_{\text{STT}} \equiv \Sigma(\lambda_{\text{ST}(i)})$$

$$\lambda_{\text{LTT}} \equiv \Sigma(\lambda_{\text{LT}(i)})$$

$$\lambda_{\text{ST-LOTC-AVE}} = \frac{\Sigma(\lambda_{\text{ST}(i)} * \lambda_{\text{ST-LOTC}(i)})}{\Sigma(\lambda_{\text{ST}(i)})}$$

$$\lambda_{\text{LT-LOTC-AVE}} = \frac{\Sigma(\lambda_{\text{LT}(i)} * \lambda_{\text{LT-LOTC}(i)})}{\Sigma(\lambda_{\text{LT}(i)})}$$

These definitions apply when using the TWA approach, because that approach involves no balancing of the times spent in the various states. However, in a Markov model, the definitions given above for λ_{STT} , λ_{LTT} , $\lambda_{\text{ST-LOTC-AVE}}$, and $\lambda_{\text{LT-LOTC-AVE}}$ are not exactly correct. Although not exactly correct, they are reasonable approximations when the repair rates, μ_{ST} and μ_{LT} are much greater than the failure rates from a given ST or LT fault state (i.e., $\lambda_{\text{ST-LOTC}(i)}$ and $\lambda_{\text{LT-LOTC}(i)}$) to the LOTC state.

This is shown as follows: The single state Markov model for a typical FADEC system is shown in Figure 10, repeated here as:

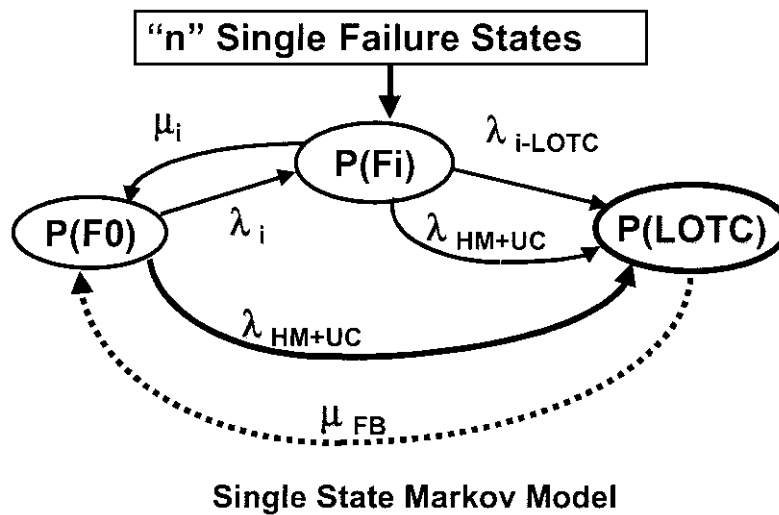


Figure E1

All " n " states are included in the model in the manner as shown in the example given in 7.4. Hence, the model will have many states, some of them will be short time (ST) states, some will be long time (LT) states, and some may be no dispatch (ND) states. Since ND states usually require two failures, and since a single failure state model is generally an adequate representation of the system, the following discussion assumes that ND states are not included. The model will of course include a full-up and an LOTC state. A single state MM, showing the ST and LT repair states would look like:

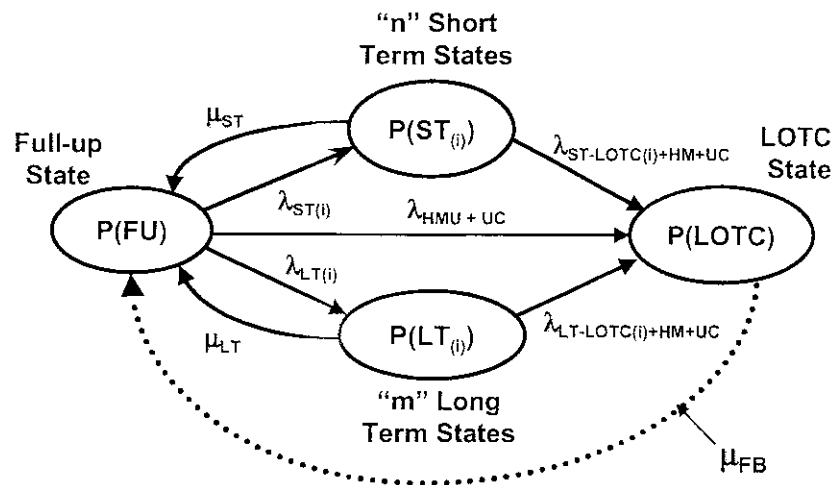
MM Diagram with " n " Short Term States and " m " Long Term States

Figure E2

The LOTC rate for this model is represented by Equation 19, given in Section 7, as:

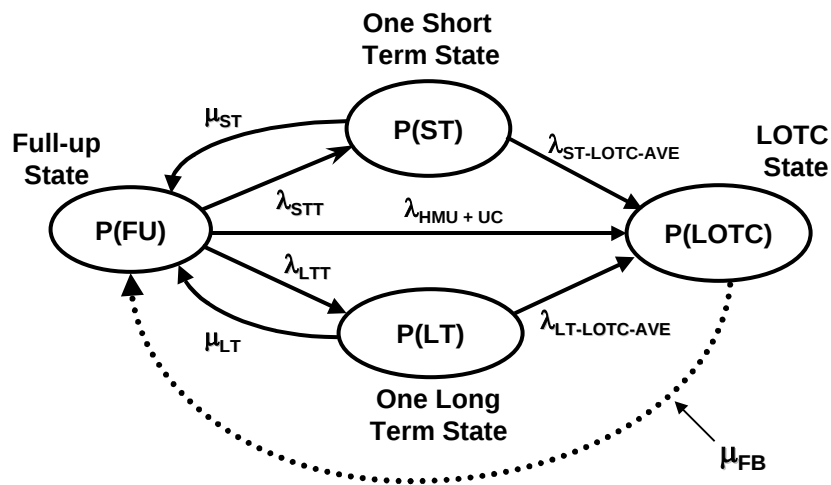
$$\lambda_{LOTG} = \frac{\lambda_{HM+UC} + \sum \{ (\lambda_i * (\lambda_{i-LOTG(i)} + HM+UC)) / (\mu_i + \lambda_{i-LOTG(i)} + HM+UC) \}}{1.0 + \sum \{ \lambda_i / (\mu_i + \lambda_{i-LOTG(i)} + HM+UC) \}} \quad (\text{Eq. E2})$$

When using the ST and LT subscript nomenclatures, this equation can be written as:

$$\lambda_{\text{LOT C}} = \frac{\lambda_{\text{HM+UC}} + \sum \{ (\lambda_{\text{ST}(i)} * \lambda_{\text{ST-LOT C}(i)} + \text{HM+UC}) / (\mu_{\text{ST}} + \lambda_{\text{ST-LOT C}(i)} + \text{HM+UC}) \} + \sum \{ (\lambda_{\text{LT}(i)} * \lambda_{\text{LT-LOT C}(i)} + \text{HM+UC}) / (\mu_{\text{LT}} + \lambda_{\text{ST-LOT C}(i)} + \text{HM+UC}) \}}{1.0 + \sum \{ \lambda_{\text{ST}(i)} / (\mu_{\text{ST}} + \lambda_{\text{ST-LOT C}(i)} + \text{HM+UC}) \} + \sum \{ \lambda_{\text{LT}(i)} / (\mu_{\text{LT}} + \lambda_{\text{ST-LOT C}(i)} + \text{HM+UC}) \}} \quad (\text{Eq. E3})$$

This type of single state MM is generally not reduced to the simplified model discussed below, where all ST fault states and all LT fault states have been combined into a single ST and LT state, respectively, using the equations for, λ_{STT} , λ_{LTT} , $\lambda_{\text{ST-LOT C-AVE}}$, and $\lambda_{\text{LT-LOT C-AVE}}$ given above. The reason for this is that the equations given above do not balance the times that the system will spend in the various states.

If, for some reason, the analysis wants to reduce the “n” ST and “M” LT state model to one which has a single “average” ST and LT state, the model would look as follows:



Simplified MM Diagram where all ST and LT Fault States are combined into a single ST and LT state

Figure E3

The LOTC rate for this model is:

$$\lambda_{\text{LOT C}} = \frac{\lambda_{\text{HM+UC}} + \frac{(\lambda_{\text{STT}} * \lambda_{\text{ST-LOT C-AVE}})}{(\mu_{\text{ST}} + \lambda_{\text{ST-LOT C-AVE}})} + \frac{(\lambda_{\text{LTT}} * \lambda_{\text{LT-LOT C-AVE}})}{(\mu_{\text{LT}} + \lambda_{\text{LT-LOT C-AVE}})}}{1.0 + \frac{\lambda_{\text{STT}}}{(\mu_{\text{ST}} + \lambda_{\text{ST-LOT C-AVE}})} + \frac{\lambda_{\text{LTT}}}{(\mu_{\text{LT}} + \lambda_{\text{LT-LOT C-AVE}})}} \quad (\text{Eq. E4})$$

In comparing Equation E4 with Equation E3, we see that for Equation E4 to be correct:

$$\frac{(\lambda_{\text{STT}} * \lambda_{\text{ST-LOT C-AVE}})}{(\mu_{\text{ST}} + \lambda_{\text{ST-LOT C-AVE}})} = \sum \{ (\lambda_{\text{ST}(i)} * (\lambda_{\text{ST-LOT C}(i)} + \text{HM+UC})) / (\mu_{\text{ST}} + \lambda_{\text{ST-LOT C}(i)} + \text{HM+UC}) \} \quad (\text{Eq. E5})$$

and

$$\frac{\lambda_{STT}}{(\mu_{ST} + \lambda_{ST-LOTC-AVE})} = \frac{\sum \{ \lambda_{ST(i)} / (\mu_{ST} + \lambda_{ST-LOTC(i)} + HM + UC) \}}{(\mu_{ST} + \lambda_{ST-LOTC-AVE})} \quad (\text{Eq. E6})$$

These are readily solved to yield:

$$\lambda_{STT} = \mu_{ST} * \frac{\sum (\lambda_{ST(i)} / (\mu_{ST} + \lambda_{ST-LOTC(i)} + HM + UC))}{1 + \sum ((\lambda_{ST(i)} * \lambda_{ST-LOTC(i)} + HM + UC) / (\mu_{ST} + \lambda_{ST-LOTC(i)} + HM + UC))} \quad (\text{Eq. E7})$$

$$\lambda_{ST-LOTC-AVE} = \frac{\sum ((\lambda_{ST(i)} * \lambda_{ST-LOTC(i)} + HM + UC) / (\mu_{ST} + \lambda_{ST-LOTC(i)} + HM + UC))}{\sum (\lambda_{ST(i)} / (\mu_{ST} + \lambda_{ST-LOTC(i)} + HM + UC))} \quad (\text{Eq. E8})$$

And similarly, the LT state terms are:

$$\lambda_{LTT} = \mu_{LT} * \frac{\sum (\lambda_{LT(i)} / (\mu_{LT} + \lambda_{LT-LOTC(i)} + HM + UC))}{1 + \sum ((\lambda_{LT(i)} * \lambda_{LT-LOTC(i)} + HM + UC) / (\mu_{LT} + \lambda_{LT-LOTC(i)} + HM + UC))} \quad (\text{Eq. E9})$$

$$\lambda_{LT-LOTC-AVE} = \frac{\sum ((\lambda_{LT(i)} * \lambda_{LT-LOTC(i)} + HM + UC) / (\mu_{LT} + \lambda_{LT-LOTC(i)} + HM + UC))}{\sum (\lambda_{LT(i)} / (\mu_{LT} + \lambda_{LT-LOTC(i)} + HM + UC))} \quad (\text{Eq. E10})$$

where:

$\lambda_{ST(i)}$ is the failure rate for a particular ST fault

$\lambda_{LT(i)}$ is the failure rate for a particular LT fault

$\lambda_{ST-LOTC(i)} + HM + UC$ is the failure rate to the LOTC state when operating with the particular ST fault, including the hydromechanical and undetected fault rate

$\lambda_{LT-LOTC(i)} + HM + UC$ is the failure rate to the LOTC state when operating with the particular LT fault, including the hydromechanical and undetected fault rate

μ_{ST} and μ_{LT} are the repair rates for the ST and LT fault states, respectively

The equations for the above terms will give the correct, balanced answer for a single ST and LT state model, but as can be seen, calculating these terms is probably more difficult than simply solving the n-state MM in its original form. Hence, MMs are rarely, if ever, simplified to having single ST and LT states that represent all ST and LT faults.

Additionally, another reason for not combining all ST and LT fault states into a single ST and LT state is that the analyst will lose sight of which ST and LT faults have the most significant impact on the system.

It is interesting to note that for

$$\mu_{ST} \gg \lambda_{ST-LOTC(i)} + HM + UC \quad \text{and} \quad \mu_{LT} \gg \lambda_{LT-LOTC(i)} + HM + UC$$

which are generally reasonable approximations, that

$$\lambda_{STT} \approx \sum (\lambda_{ST(i)})$$

$$\lambda_{ST-LOTC-AVE} \approx \frac{\sum (\lambda_{ST(i)} * \lambda_{ST-LOTC(i)} + HM + UC)}{\sum (\lambda_{ST(i)})}$$

and

$$\lambda_{LTT} \approx \sum (\lambda_{LT(i)})$$

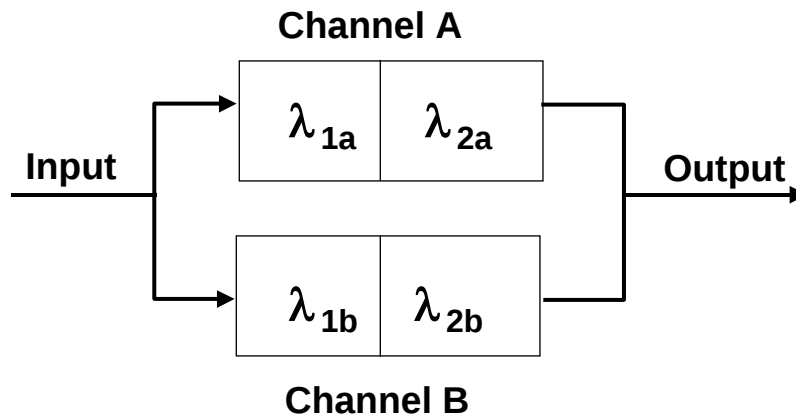
$$\lambda_{LT-LOTC-AVE} \approx \frac{\sum (\lambda_{LT(i)} * \lambda_{LT-LOTC(i)} + HM + UC)}{\sum (\lambda_{LT(i)})}$$

These are the same approximations used in the TWA equations at the beginning of this Appendix. Again, however, when these summations are done, it will not be as easy to see what fault states are the significant influences on the overall LOTC rate. Hence, it is recommended that nearly all of the single fault states, both ST and LT states, are retained as separate states in the model, as was done in the example given in 7.4.

APPENDIX F - WHEN IS A SINGLE STATE MODEL OK?

The question often arises: “Why is a single state model OK?”

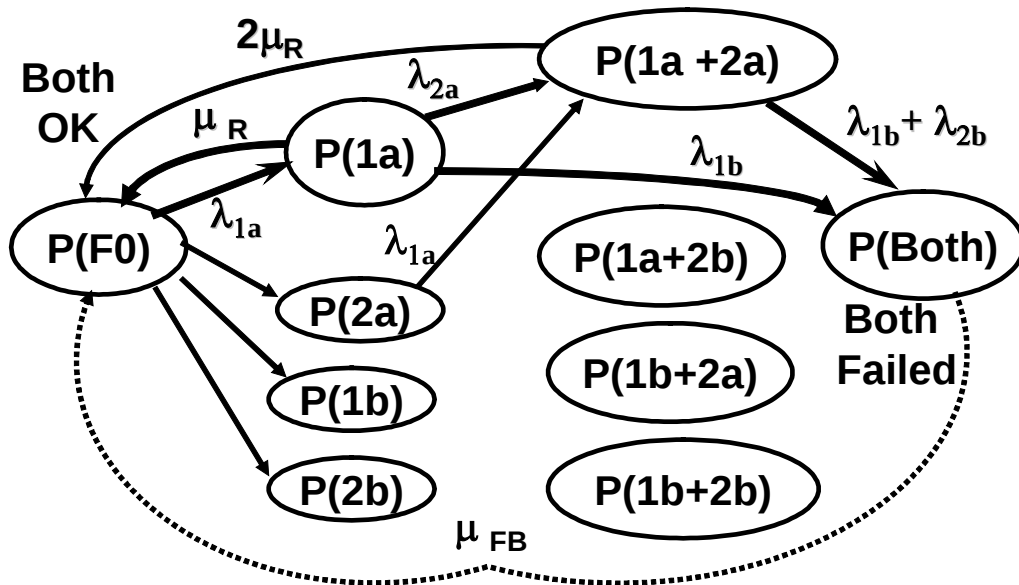
To illustrate why a single state model is generally adequate, consider the following system:



Simple Dual Element System Diagram

Figure F1

Assume the model has four single failure states representing the elements 1a, 1b, 2a, and 2b. Further assume, just for the purposes of this example, that the system needs a “healthy” #1 and #2 element to be operate. If this were the case, the system could operate with combination of elements (1a and 2a), (1b and 2b), (1a and 2b), or (1b and 2a) failed. The Markov model for this system is shown in the figure below.



Closed Loop MM Model with 2nd. Order States

Figure F2

This model diagram is simplified in that it only shows the transitions into the single fault, P(1a) state, and the dual fault, P(1a+2a) state. The transitions into the other single and dual fault states are similar, but the diagram becomes cluttered when they are shown, and they are not needed for this explanation.

The probability flow into the P(Both) state is:

$$\text{Probability flow into P(Both)} = \lambda_{1b} * P(1a) + \{ \lambda_{1b} + \lambda_{2b} \} * P(1a+2a) \quad (\text{Eq. F1})$$

+ those six other (similar) terms; one from each of the three other single failure states, and one from each of the three other dual failure states.

The probability flow equation for the state, P(1a + 2a) can be arranged to yield:

$$P(1a + 2a) = \{ \lambda_{1a} * P(2a) + \lambda_{2a} * P(1a) \} / \{ \lambda_{1b} + \lambda_{2b} + 2 * \mu_R \} \quad (\text{Eq. F2})$$

Substituting the above P(1a + 2a) equation into the probability flow Equation F1 yields:

$$\text{Probability flow into P(Both)} = \lambda_{1b} * P(1a) + \frac{\{ \lambda_{1b} + \lambda_{2b} \} * \{ \lambda_{1a} * P(2a) + \lambda_{2a} * P(1a) \}}{\{ \lambda_{1b} + \lambda_{2b} + 2 * \mu_R \}} \quad (\text{Eq. F3})$$

+ those six other (similar) terms; one from each of the three other single failure states, and one from each of the three other dual failure states.

$$\begin{aligned} \text{Probability flow into P(Both)} = & \left\{ \lambda_{1b} + \frac{\lambda_{2a} * (\lambda_{1b} + \lambda_{2b})}{\lambda_{1b} + \lambda_{2b} + 2 * \mu_R} \right\} * P(1a) + \\ & + \left\{ \frac{\lambda_{1a} * (\lambda_{1b} + \lambda_{2b})}{\lambda_{1b} + \lambda_{2b} + 2 * \mu_R} \right\} * P(2a) \end{aligned} \quad (\text{Eq. F4})$$

+ those six other (similar) terms; one from each of the three other single failure states, and one from each of the three other dual failure states.

Now, examine the P(1a) coefficient:

$$\lambda_{1b} + \frac{\lambda_{2a} * (\lambda_{1b} + \lambda_{2b})}{\lambda_{1b} + \lambda_{2b} + 2 * \mu_R}$$

For a first order model to be reasonably representative of the system, the second term in the above coefficient must be small in comparison to the first term. This will be the case if μ_R is much greater than any of the failure rates λ_{1a} , λ_{2a} , λ_{1b} , and λ_{2b} .

In general, μ_R should be 10 times greater than the highest failure rate into or out of all failure states that are in a given group or category, such as the ST or LT fault group. In our particular example of the Appendix, assume all of the failure rates are approximately the same. If this is the case, then the maximum failure rates will be those leaving the dual failure states. These rates will be the sum of two failure rates, such as $(\lambda_{1b} + \lambda_{2b})$.

If μ_R is established so that:

$$\mu_R > 10 * (\lambda_{1b} + \lambda_{2b})$$

Then the P(1a) coefficient reduces to:

$$\lambda_{1b} + \text{a number less than } \left(\frac{\lambda_{2a}}{10} \right)$$

And if all of the single failure rates, λ_{1a} , λ_{2a} , λ_{1b} , and λ_{2b} are approximately the same order of magnitude, which they generally are in a FADEC system model, the second term, which comes from a dual failure state will add less than approximately 10% to the first term. This is adequate accuracy for the model. The component failure rate data used in the model is probably not that accurate.

APPENDIX G - COMPARISON OF THE ASYMPTOTIC VALUE OF $\{(dP/dt)/(1 - P)\}$ IN AN OPEN LOOP MARKOV MODEL WITH THAT OF THE AVERAGE FAILURE RATE OF THE SYSTEM FROM A CLOSED LOOP MARKOV MODEL

Consider the following system:

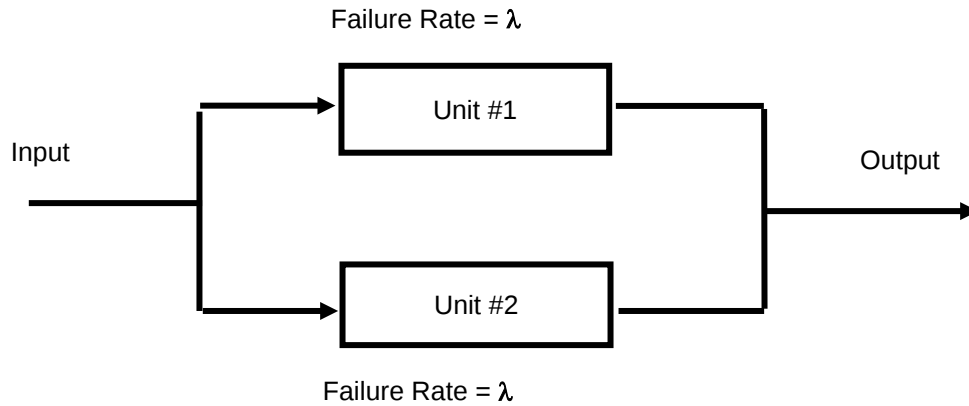


Figure G1 - Simple 2-unit system

The open loop Markov model for the system is:

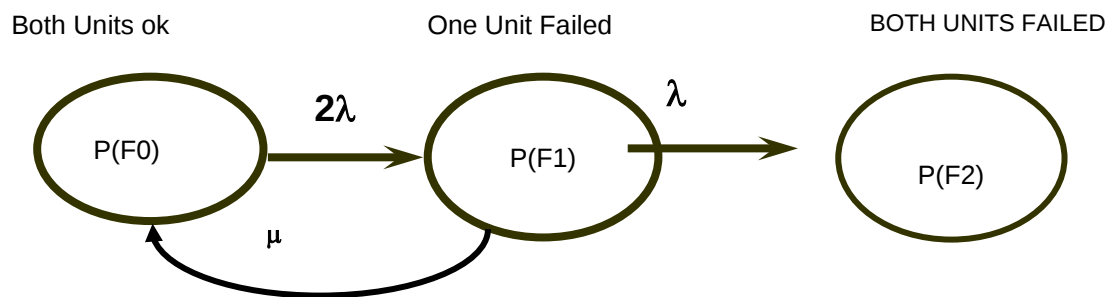


Figure G2 - Open loop Markov model of 2-unit system with repair

where:

$P(F_0)$ is the probability of both unit operative

$P(P_1)$ is the probability of having one unit failed

$P(F_2)$ is the probability of both units being failed

The differential equations representing the system are:

$$dP(F_0)/dt = -2\lambda P(F_0) + \mu P(F_1)$$

$$dP(F_1)/dt = 2\lambda P(F_0) - (\lambda + \mu)P(F_1)$$

$$dP(F_2)/dt = \lambda P(F_1)$$

Starting with the initial condition, $P(F0) = 1$ and $P(F1) = P(F2) = 0$, these equations are solved to yield:

$$\begin{aligned} P(F0) &= [(\lambda - \mu + x) e^{-(3\lambda + \mu + x)t/2} + (-\lambda + \mu + x) e^{-(3\lambda + \mu - x)t/2}] / (2x) \\ P(F1) &= [(-4\lambda) e^{-(3\lambda + \mu + x)t/2} + (4\lambda) e^{-(3\lambda + \mu - x)t/2}] / (2x) \\ P(F2) &= 1.0 + [(3\lambda + \mu - x) e^{-(3\lambda + \mu + x)t/2} + (-3\lambda - \mu - x) e^{-(3\lambda + \mu - x)t/2}] / (2x) \end{aligned}$$

$$\text{Where } x = + (\lambda^2 + 6\mu\lambda + \mu^2)^{0.5}$$

The average failure rate of the system is estimated from $[dP(F2)/dt]/[1-P(F2)]$ as $t \rightarrow \infty$. From the above equations, this is determined to be:

$$4\lambda^2 / (3\lambda + \mu) \quad (\text{Eq. G1})$$

Now consider the same system with a closed loop Markov model. The model is:

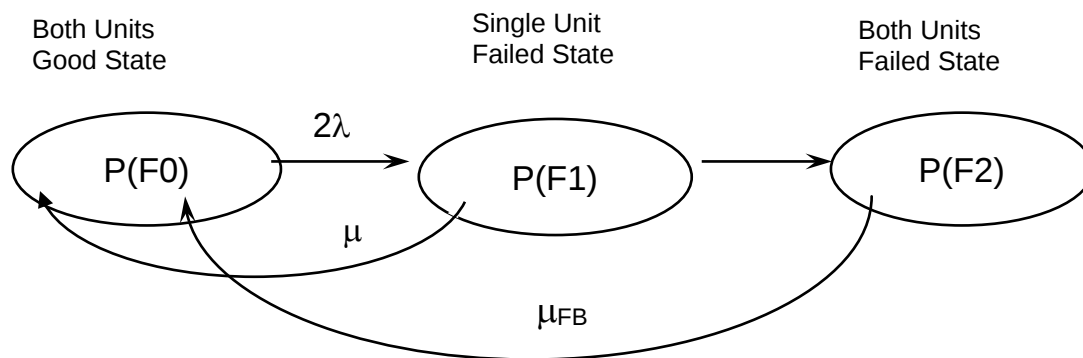


Figure G3 - Closed loop Markov model of 2-unit system

The steady state solution is obtained by solving the algebraic set of equations:

$$\begin{aligned} 1 &= P(F0) + P(F1) + P(F2) \\ 0 &= -\lambda * P(F0) - (\lambda + \mu) * P(F1) \\ 0 &= \lambda * P(F1) - \mu_{FB} * P(F2) \end{aligned}$$

The solution is:

$$\begin{aligned} P(F0) &= \mu_{FB} * (\lambda + \mu) / D \\ P(F1) &= 2\lambda \mu_{FB} / D \\ P(F2) &= 2\lambda^2 / D \\ D &= 2\lambda^2 + 3\lambda \mu_{FB} + \mu * \mu_{FB} \end{aligned}$$

The average (steady state) LOTC rate for the system is given by:

$$2\lambda^2 / (3\lambda + \mu) \quad (\text{Eq. G2})$$

The open loop failure rate from Equation G1 is shown with the closed loop (average) failure rate of the system in Figure G4.

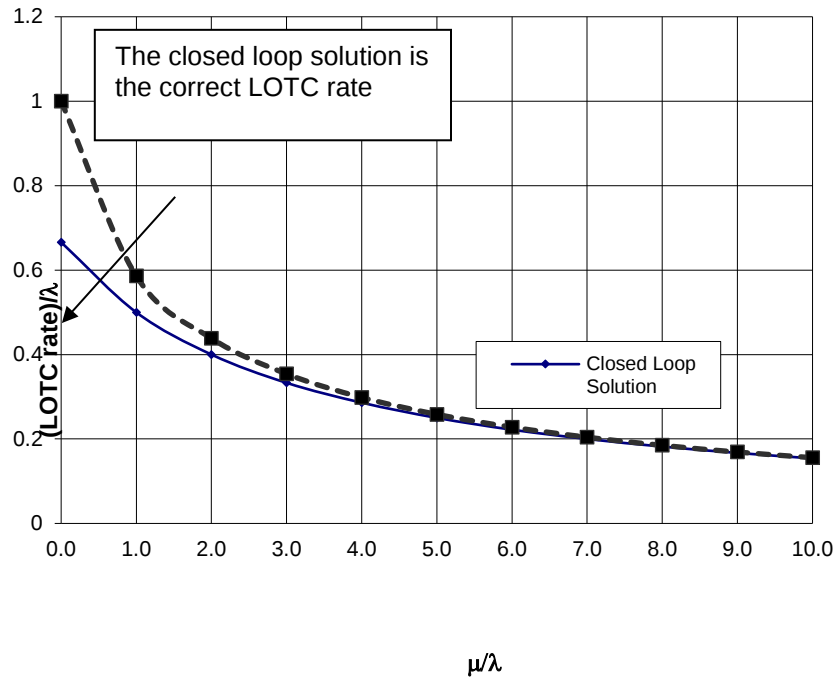


Figure G4 - Comparison of the Asymptotic open loop MM failure rate with the closed loop (average) MM failure rate for the 2-unit system

NOTE: In Figure G4, the error in the asymptotic value for the LOTC rate can be considerable when the repair rates are close to zero (i.e., no repair), but the error becomes quite small for repair rates that are at least 10 times the failure rate, λ , of the units. The possibility of the error is one of the reasons that closed loop models are preferred.